



3 1761 11709023 3

A1
S 73
133

Government
Publications

Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada

Privacy

Annual Report
to Parliament
2004-2005
Report on the
Privacy Act

Canada

Privacy Commissioner
of Canada

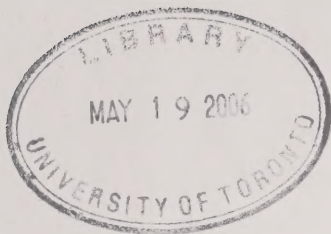


Commissaire à la protection
de la vie privée du Canada

Privacy

**Annual Report
to Parliament
2004-2005**
Report on the
Privacy Act

Canada



Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2005
Cat. No. IP50-2005
ISBN 0-662-68763-9

This publication is also available on our Web site at www.privcom.gc.ca, in addition to our 2004 Annual Report on the *Personal Information Protection and Electronic Documents Act*.

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



October 2005

The Honourable Daniel Hays, Senator
The Speaker
The Senate of Canada
Ottawa


Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2004 to March 31, 2005.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761117090233>

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



October 2005

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2004 to March 31, 2005.

Yours sincerely,

A handwritten signature in dark ink that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Foreword1

Our Multi-Faceted Mandate5

Policy Perspective.....7

 Parliament’s Window on Privacy.....7

 National Security10

Anti-terrorism Act11

 Transborder Flows of Personal Information.....11

 Integrating Information Systems12

 The Impact of the *USA PATRIOT Act*.....13

 The Canada Border Services Agency Audit15

Privacy Act Reform17

 How We Got Here18

 The New National Security Paradigm.....19

 Transborder Data Flows19

 Government On-Line or “E-Government”20

 Extending the Scope of the *Privacy Act*21

Privacy Management Framework	27
Building a Privacy Management Framework for the Federal Government	27
Complaints.....	33
Introduction	33
Investigations and Inquiries	34
Complaints Received	34
Complaints Completed	38
Definitions of Findings under the <i>Privacy Act</i>	39
Investigation Process under the <i>Privacy Act</i>	44
Select Cases under the <i>Privacy Act</i>	47
Incidents under the <i>Privacy Act</i>	55
Public Interest Disclosures under the <i>Privacy Act</i>	57
Inquiries	58
Audit and Review	61
Strengthening the Audit Function	61
Auditing Cross-Border Flow of Personal Information	62
Other Audit and Review Activity	64
In the Courts	69
<i>Privacy Act</i> Applications	69
Judicial Review	71
Public Education and Communications	73
Corporate Services	77
On the Path to Institutional Renewal	77
Financial Information	81

Foreword



If Canada had optimal privacy protection, the Annual Reports from the Office of the Privacy Commissioner would be a detailed account of successful interventions to protect the rights of individuals, of audits of well run federal institutions with mature business processes incorporating privacy requirements, and a thorough policy analysis of new information systems and technologies. Instead, reports from this office have too often lamented the steady erosion of rights and the assault of new surveillance technologies on the daily lives of Canadians, and our impotence to reverse the trends.

This year is no exception. Increasingly, the phenomenon of outsourcing and public-private partnerships means the data of Canadians may be in the hands of the private sector even when under the control of the government.

We are generally pleased with the results of our interventions, and with the cooperation of business and government alike to try to comply with fair information practices and legal requirements, but the privacy threats seem to be multiplying like a bad virus, threatening to overwhelm us.

If there is one central message we want to convey this year, it is that we are not going to allow that to happen. We mean business, and we are counting on the support of all institutions to help us grapple with these issues and preserve and maintain the privacy of the individuals in this country.

Canadians are anxious, and they expect us to enforce the law and their government to respect the values inherent in our Constitution, as recent polling data shows. We will do our part, but the defence of these fundamental rights of information protection demands a shift in public policy such as has started to take place with respect to the

environmental movement. Over the last twenty years it has become well accepted that it is not alright to pollute, that it is expected behaviour to recycle. We need the same thing to happen with respect to personal information: it is not alright to gather information without consent, it is not alright to share it promiscuously, it is not alright to hide your information practices from your public.

Three main themes will be found throughout this report, because they are the most significant issues we have faced: security and the voracious appetite for personal information and surveillance that has sprung up in the post-911 environment, sharing of information and outsourcing of data operations across borders, and the need to modernize our *Privacy Act*. Whether you read this report as an individual member of the public, a public servant, or a Parliamentarian, there is a message we want to convey to you:

Start caring about privacy now, before it is too late. Citizens' involvement in the debate will determine the course our country takes with regard to the protection of personal information. Do your part to control the flow of everyone's personal information. We are here to help, but we cannot do the job alone.

This year, we have published two separate reports, dividing the Privacy Act from the Personal Information Protection and Electronic Documents Act (PIPEDA). We felt this was more appropriate given that the Privacy Act requires us to report on the fiscal year (2004–2005), while under PIPEDA we are required to report on the calendar year (2004). As well, each Act provides a separate framework for investigations and audits. Both our reports detail efforts we have taken to meet the growing demands on our Office to act as the guardians of privacy for Canadians on behalf of Parliament. There is much overlapping between these reports because many of our activities are not particular to one law or another and, increasingly, the policy issues are common across the two regimes.

Our Multi-Faceted Mandate

The Office of the Privacy Commissioner (OPC), oversees both the *Privacy Act*, which applies to federal institutions, and *PIPEDA* which governs personal information management in commercial activities in the private sector.

Parliament has given the Office a mandate to ensure that both the federal public sector and private sector (in most provinces) are held accountable for their personal information handling and that the public is informed about their privacy rights. The mandate is not always understood.

As an independent ombudsman, we are:

- An *investigator* and *auditor* with full powers to investigate and initiate complaints, conduct audits and verify compliance under both Acts;
- A *public educator* and *advocate* with a responsibility both to sensitize businesses about their obligations under *PIPEDA* and to help the public better understand their data protection rights;
- A *researcher* and *expert adviser* on privacy issues to Parliament, government and businesses; and
- An *advocate for privacy principles* involved in litigating the application and interpretation of the two privacy laws. We also analyze the legal and policy implications of bills and government proposals.

Although the *Privacy Act* does not give the Privacy Commissioner a formal legal mandate to conduct public education, the Commissioner often needs to inform the public and government in order to achieve her mandate to hold federal government departments and agencies accountable for their personal information-handling practices.

Policy Perspective

Parliament's Window on Privacy

The Privacy Commissioner of Canada is an Agent of Parliament who reports directly to the Senate and the House of Commons. As such, the OPC acts as Parliament's window on privacy issues. Through the Commissioner, Assistant Commissioners and other senior OPC staff, the Office brings to the attention of Parliamentarians issues that have an impact on the privacy rights of Canadians. The OPC does this by tabling Annual Reports to Parliament, by appearing before Committees of the Senate and the House of Commons to comment on the privacy implications of proposed legislation and government initiatives, and by identifying and analyzing issues that we believe should be brought to Parliament's attention.

The Office also assists Parliament in becoming better informed about privacy, acting as a resource or centre of expertise on privacy issues. This includes responding to a significant number of inquiries and letters from Senators and Members of Parliament.

➤ *Appearances before Parliamentary Committees*

Appearances before committees of the Senate and the House of Commons constitute a key element of our work as Parliament's window on privacy issues. During the period covered by this report, the Privacy Commissioner and other senior OPC staff appeared 11 times before Parliamentary committees: six times on bills with privacy implications; four times on matters relating to the management and operations of the Office; and once before a Senate committee studying consumer issues in the financial services sector.

The OPC appeared on the following bills before Parliamentary committees in 2004-2005:

- Bill C-2, *An Act to Amend the Radiocommunication Act* (May 6, 2004)
- Bill C-12, the *Quarantine Act* (November 18, 2004)
- Bill C-22, *An Act to establish the Department of Social Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-23, *An Act to establish the Department of Human Resources and Skills Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-11, the *Public Servants Disclosure Protection Act* (December 14, 2004)
- Bill C-13, *An Act to Amend the Criminal Code, the DNA Identification Act and the National Defence Act* (February 8, 2005)
- Bill S-18, *An Act to Amend the Statistics Act* (February 24, 2005)

Regarding the management and operations of the Office, OPC officials appeared before Parliamentary committees on the following matters in 2004-2005:

- Annual Report and Main Estimates 2003-2004 (November 17, 2004)
- Supplementary Estimates (December 1, 2004)
- Funding mechanisms for Agents of Parliament (February 10, 2005)
- Role and operations of the OPC (February 16, 2005)

► *Other Parliamentary Liaison Activities*

The OPC has undertaken a number of other initiatives over the course of the past year to improve its ability to advise Parliament on privacy matters.

In May 2004, we created a dedicated Parliamentary liaison function within the Office to improve our relationship with Parliament. This function resides in the Research and Policy Branch, reflecting the OPC's desire to focus its Parliamentary affairs activities on providing in-depth and accurate policy advice to Senators and Members of Parliament.

Improving on how we assess, monitor and forecast Parliamentary activity has been a priority for us in the past year. The OPC put in place a new and improved system for monitoring the status of bills on Parliament Hill, as well as keeping tabs on new and emerging developments of interest to privacy promotion and protection. Our goal is to build bridges to departments so that we can comment earlier in the legislative process, when our criticisms could be dealt with more effectively. It is often too late

when a bill has been introduced in the House of Commons, to rethink approaches to information issues.

The Office has responded to a significant number of inquiries and letters from Senators and MPs this year, and the Commissioner and Assistant Commissioners have also met privately with Senators and MPs who wished to discuss policy matters relating to privacy, or wanted to know more about the operations of the Office.

In late 2004, the OPC, in conjunction with the Office of the Information Commissioner, and in collaboration with the Research Branch of the Library of Parliament, held an information session for Parliamentarians and their staff on the roles and mandates of both Offices. This information session was well attended and raised many questions among participants. We believe such information sessions contribute to increasing awareness of privacy issues on Parliament Hill, and look forward to holding more such sessions in the future.

► *Priorities for the Coming Year*

The Office expects to be busy in the area of Parliamentary affairs over the next fiscal year. There are a number of bills of interest to us expected in the upcoming session, and the statutory review by Parliament of the *Personal Information Protection and Electronic Documents Act* is expected to start in 2006. The OPC plans to play a constructive role during this review, by providing thoughtful advice to Parliamentarians mandated with studying at how the Act has worked over the course of its first years of implementation, and how it may be modified and improved.

The OPC will continue to follow with interest the Parliamentary review of the *Anti-terrorism Act*. The Privacy Commissioner appeared twice before committee on this matter in fiscal year 2005-06—once before a Senate special committee reviewing the Act (May 9, 2005), and on another occasion before a sub-committee of the Commons Standing Committee on Justice (June 1, 2005).

We recognize that to act as an effective Agent of Parliament we need to have good working relationships with federal departments and agencies. The OPC plans to put more emphasis on identifying and raising privacy concerns when government initiatives are being developed rather than waiting until they reach Parliament, as this increases the possibility that privacy concerns will be taken into account.

National Security

In May 2004 Parliament passed the *Public Safety Act*. The Act, originally introduced in November 2001 in the wake of the September 11 terrorist attacks, allows the Minister of Transport, the Commissioner of the Royal Canadian Mounted Police (RCMP) and the Director of the Canadian Security Intelligence Service (CSIS) to compel, without a warrant, air carriers and operators of aviation reservation systems to provide information about passengers. While this may seem reasonable given the risks terrorists pose to air transport, authorities are not using this information exclusively for anti-terrorism and transportation safety. The *Public Safety Act* also allows law enforcement authorities to use the information to identify passengers with outstanding arrest warrants for a wide range of ordinary criminal offences. In other words, the machinery of anti-terrorism is being used to meet the needs of ordinary law enforcement, lowering the legal standards that law enforcement authorities in a democratic society must meet.

Another provision in the *Public Safety Act* amends *PIPEDA* to allow private sector institutions to collect personal information, without clients' consent, and disclose it to government, law enforcement and national security agencies. The amendment applies not just to transportation companies but to any institution subject to *PIPEDA*—financial institutions, telecommunications companies and retailers. These disclosures effectively co-opt private sector institutions, pressing them into the service of law enforcement activities and dangerously blurring the line between the private sector and the state.

Not only is the private sector being deputized by law enforcement; an anti-terrorism mindset is permeating more conventional law enforcement and public safety initiatives. This mindset threatens to erode our privacy rights and other freedoms because the constraints under which national security agencies operate—for example, the requirement for judicial authorization—are often weaker than those governing law enforcement agencies.

Debates about public safety are nothing new. They have been underway for several years, certainly before 9/11. However, we now hear explicit messages about “intelligence-based policing” and vigilance to prevent terrorism from taking hold in our society. The proliferation of these messages without an equal attention to the need to protect civil liberties is of concern. Implicit in the debate is a general acceptance of various types of surveillance, and a marked shift towards the reduction of our civil liberties. A state which routinely accepts threats to civil liberties and Charter-protected autonomy rights is on spongy ground.

While our society must deal with legitimate security concerns, we must also guard against fear-mongering and intolerance which threaten a liberal democracy.

Anti-terrorism Act

The *Anti-terrorism Act* (passed in the fall of 2001) requires a Parliamentary review after three years. The Senate has appointed a Special Committee to conduct its review while the House of Commons has referred the review to the Public Safety and National Security Subcommittee of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness.

In participating in this review, we define the most important questions for the review to be: Are the additional law enforcement and surveillance powers necessary and proportional to the threats they were intended to address? Have the security benefits justified the sacrifice of privacy and other rights?

We face several challenges preparing for the review, one of which is trying to determine whether the extraordinary powers the *Anti-terrorism Act* granted law enforcement and national security agencies are really needed and effective. We have found no empirical assessments of their effectiveness in detecting, preventing or deterring terrorist acts. Our challenge is compounded by government simultaneously granting new powers to law enforcement and national security agencies while weakening transparency and accountability.

The *Anti-terrorism Act* cannot be viewed in isolation. In the Spring of 2005 we urged the two Committees reviewing the Act to interpret their mandates broadly, examining the cumulative impact on Canadians' privacy rights of all the measures passed in the wake of the September 11 attacks—amendments to the *Aeronautics Act* (passed in late 2001), the Public Safety Act and the *Immigration and Refugee Protection Act*.

Transborder Flows of Personal Information

The *Anti-terrorism Act* is by no means the only government initiative that threatens privacy. Government is collecting, analyzing and sharing more personal information helped along by improved technology, new legislation, government reorganization, and greater co-operation with foreign states. Flows of personal information are likely to have increased significantly among government departments and agencies both within and outside Canada.

All these factors have fundamentally shifted the relationship between national security, law enforcement and informational privacy with a corresponding loss of privacy and due process protections for individuals.

In April 2004, the government issued its first-ever National Security Policy. The Policy promised to create an “Integrated Threat Assessment Centre” to help collect, analyze and share intelligence and other information—effectively contributing to a more integrated international intelligence community. This Centre is housed in CSIS but staffed by employees from several departments and agencies.

Government has been reorganized; creating a new Department of Public Safety and Emergency Preparedness Canada, and new agencies such as the Canada Border Services Agency (CBSA). Reorganization will intensify information sharing among what were once separate entities.

Some have cited the *Privacy Act* as a barrier to sharing critical personal information. The *Privacy Act* does not need to be reformed, to facilitate information sharing—that is already possible. It needs to be reformed to counter the greater surveillance and the intensive transactional data collection we now see.

Privacy Act reform is not a new idea. Calls for reform date back to the late 1980s, long before the advent of today’s surveillance and information technologies. Instead of strengthening the Act, the Government has weakened its provisions by measures such as those in the *Anti-terrorism Act*.

Integrating Information Systems

Even less visible has been the government’s investment in integrated information systems that collect and analyze significant amounts of personal information about our travel patterns, financial transactions, and even in some cases the people with whom we associate. The systems analyze and mine the personal data in an attempt to find patterns that might suggest an individual is a security threat, a money launderer or is financing a terrorist group.

As law enforcement and national security agencies collect more information, from more sources, about more individuals, the probability increases that authorities will make decisions based on information of questionable accuracy or take information out of context. Misuse, misinterpretation or improper disclosures of personal information can have serious adverse consequences for individuals, families, and even communities.

The problem is aggravated when secrecy provisions and a lack of transparency prevent us from determining where the system broke down or why individuals were wrongly targeted.

Not surprisingly, the new “Smart Border” approach to border security has increased co-operation and information sharing with the United States. For example, both countries have created Integrated Border Enforcement Teams and Integrated Marine Enforcement Teams of law enforcement agencies to co-ordinate efforts to target cross-border criminal and terrorist activities.

Increasingly though, Canadians are concerned about information sharing with the United States, particularly given American federal departments’ and agencies’ lack of oversight on the collection, use and disclosure of personal information. In addition, the United States *Privacy Act of 1974* does not apply to foreign nationals, thereby depriving Canadians and citizens of other countries of certain privacy protections—including access and redress rights—under U.S. law. An EKOS Research Associates survey commissioned by our Office in March 2005, found 85 per cent of those surveyed reporting a moderate or high level of concern about Canadian government agencies transferring personal information to foreign governments to protect national security.

The Impact of the *USA PATRIOT Act*

These concerns have been highlighted by a provision in the *USA PATRIOT Act* (Section 215) that allows a special court to secretly issue an order requiring “the production of any tangible things”, possibly including an individual’s personal information, to the Federal Bureau of Investigation (FBI). The Act also prohibits anyone served with such a secret order from disclosing that they have complied with it, or even that it exists.

In 2004 the British Columbia Information and Privacy Commissioner, David Loukidelis, announced that he was examining whether “the *USA PATRIOT Act* permit[s] United States authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of USA-linked private sector service providers.”

The B.C. Commissioner began the review following a proposal that a Canadian subsidiary of an American company take over administration of the province’s Medical Services Plan and PharmaCare programs. Critics of the proposal argued

that that this could potentially allow American agencies such as the FBI to obtain personal information about Canadians from the American company under the *USA PATRIOT Act*.

In August 2004, we made a submission to the B.C. Commissioner entitled “Transferring Personal Information about Canadians Across Borders —Implications of the *USA PATRIOT Act*”. The submission explained that a company holding personal information about Canadian residents in Canada would not be required to provide this information to a foreign government or agency in response to a court order, even if the company was a subsidiary of a company based in the foreign country. In fact, the company would violate *PIPEDA* if it did disclose the information without the individuals’ consent. An exception would allow disclosures of information under legislation such as the 2001 amendments to the *Aeronautics Act* that allow airlines to disclose passenger information to foreign states.

PIPEDA provides further protection by requiring institutions that transfer personal information to a third party for processing to use “contractual or other means” to ensure that a company located in another country provides comparable protection of personal information to that provided in Canada.

However, our submission acknowledged that companies holding personal information about Canadians in a foreign country must comply with that country’s laws and would have to disclose personal information in response to a court order. This means that a Canadian company outsourcing its personal information processing to the United States effectively exposes the information to U.S. law.

The B.C. government responded to the controversy by passing legislation amending the *Freedom of Information and Protection of Privacy Act (FOIPPA)* and nine other Acts. The legislation places restrictions on B.C. public bodies and service providers when storing, accessing or disclosing personal information outside Canada.

Of course, the B.C. legislation does nothing to protect the personal information that the federal government transfers outside the country, nor does *PIPEDA* apply. We urged the federal government to examine the circumstances under which it allows personal information about Canadians to be processed outside Canada and to explain the nature of these transfers to Canadians. The Commissioner observed that “Canadians need to understand the full extent to which their personal information is transferred across borders and the full extent to which personal information about them can be and is made available to foreign governments and institutions”.

We followed up early in 2005 with a letter to the President of the Treasury Board urging the federal government to review the implications of its outsourcing of personal information and to develop contractual clauses to protect personal information transferred to third parties for processing.

The Canada Border Services Agency Audit

We also began planning an audit of the Canada Border Services Agency (CBSA) that will focus on its exchange of information with the United States. The audit's overall objective will be "to assess the extent to which the CBSA is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or institutions thereof". A key element will be reporting and mapping, as much as practicable, what information about Canadians CBSA transmits to the United States and for what purposes.

The audit will examine several key operational systems CBSA uses to process the personal information collected and shared with U.S. counterparts. The audit will also assess the overall robustness of CBSA's privacy management as well as how it reports its privacy management responsibilities to Parliament and the public.

In closing, the Privacy Commissioner is not opposed to fighting terrorism and improving our security; we are not opposed to information sharing. However, we must ensure that the steps we take to enhance our security do not end up weakening the freedoms that define the society we are defending. We need well-designed laws, increased oversight and accountability — and effective checks and balances.

When we diminish our rights without enhancing security, no one wins. But enhancing security without eroding legitimate privacy rights — that's a win for all.

Privacy Act Reform

This section elaborates on the situation and explains some of the important things for the government to consider in updating the *Privacy Act*; something long overdue.

The privacy landscape is infinitely more complex today than it was a decade ago. Faced with increased globalization and extensive outsourcing of personal information processing and storage, Canada's *Privacy Act* lags woefully behind.

Today's commonplace information technologies—the Internet and new surveillance technologies such as digital video, linked networks, global positioning systems, black boxes in cars, genetic testing, biometric identifiers and radio frequency identification devices (RFIDs) —did not exist when the federal *Privacy Act* came into force in 1983. Characterizing the current Act as dated in coping with today's realities is an understatement — the Act is tantamount to a cart horse struggling to keep up with technologies approaching warp speed.

New technologies designed for, or capable of, surveillance of individuals are widespread and are used not only by law enforcement and national security agencies. Businesses, individuals—even your new car—are gathering personal data using surveillance cameras, spyware, infrared heat sensors and data mining, often without your knowledge or consent.

Personal information has become a lucrative commodity. Protecting that information particularly in the public sector is an ongoing challenge for privacy advocates — one that is exacerbated by a federal *Privacy Act* that contains no effective controls on the export of personal information.

How We Got Here

As early as the 1960s, Canadians began questioning the relationship between information, privacy and political power. They began to worry that our increasing use of computers could lead to loss of individuality or enforce conformity.

In 1971, in the face of growing concerns, the Departments of Justice and then-Communications struck a joint task-force to examine the social and legal implications of computer technology. Their study produced the watershed report *Privacy and Computers* whose recommendations led to embedding privacy rights in the *Canadian Human Rights Act* in 1978.

The current *Privacy Act* built on and strengthened those rights. It also reflects privacy guidelines adopted in 1980 by the Organization for Economic Co-operation and Development (OECD), of which Canada is a member.

Canada is a signatory to several international instruments that stress the seminal importance of privacy. The *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*, both speak of the right to the protection of the law against arbitrary interference with privacy. Our own Supreme Court is gradually fleshing out a privacy right through the *Canadian Charter of Rights and Freedoms*. But faced with 21st century threats, the *Privacy Act* is now an outdated and often inadequate public sector data protection law.

It did not need to be this way. In 1987, three years after the *Privacy Act* took effect, Parliament conducted a required review and issued a comprehensive report recommending significant changes. Ten years later, another Parliamentary committee recommended a substantial overhaul. Repeated submissions and reports by Privacy Commissioners have flagged the toll technology is taking on Canadians' privacy rights.

The weaknesses are even more striking when the *Privacy Act* – a first generation data protection law – is measured against the new *Personal Information Protection and Electronic Documents Act (PIPEDA)*. In fact, several of the Office of the Privacy Commissioner's concerns could be remedied by adopting provisions similar to those in *PIPEDA*.

The New National Security Paradigm

As mentioned earlier in this report, the events of September 11, 2001 seem to have led to national security trumping all else. Of course, Canadians want to protect their own safety, as well as that of their allies. The risk—as always—is that vastly expanded surveillance systems will steadily erode our privacy (and other) rights, lower our reasonable expectation of privacy and autonomy, and ignore the critical question of where we must draw the line.

Both the *Anti-terrorism Act* and the *Public Safety Act, 2002* have established an atmosphere conducive to broader surveillance of both individuals and institutions. Much of the highly sensitive information about the lives of individuals, families and communities is stored in integrated information systems with broad access to law enforcement and security communities.

The cumulative impact of the new legislation is worrying. First, the surveillance powers of security and law enforcement agencies have been overly broadened. Second, the constraints on use of surveillance powers—including by the Court—have been unduly weakened. And finally, government accountability and transparency have been significantly reduced. We risk trying to defend our society by means that abrogate the fundamental freedoms that define it.

Transborder Data Flows

The *Privacy Act* must now grapple with a world in which “globalization” means not just international trade in goods; it also means an extensive traffic in personal information for off-shore processing and storage by both governments and the private sector. Effectively this moves the information out from under the umbrella of Canadian law and potentially into a legal vacuum.

As we noted above, there has been a steady increase in transfers of personal information from government to government, particularly since September 11, 2001, as well as from government to companies abroad. The *Privacy Act* imposes no obligations on third parties overseas which hold and process personal information about Canadians. There are now no Treasury Board policies governing government institutions on the issue, although some are being considered. While we applaud new policies, the *Privacy Act* should contain specific wording to define the responsibilities of those who transfer personal information outside the public sector and indeed, outside Canada.

Another implication of outsourcing is the exposure of Canadians' personal information to the reach of the *USA Patriot Act*, which we raised earlier in this report. Canadian and U.S. governments already have extensive information sharing agreements for law enforcement and security purposes, thus the impact on government records and transfers may be slight. However, a decision by a Canadian government institution or company to process and store customer data in the U.S. would now expose the information to U.S. agencies, effectively nullifying the protection provided by both the *Privacy Act* and *PIPEDA*.

Government On-Line or "E-Government"

The *Privacy Act* must also struggle with pressures from government agencies—and the public, it must be said—to deliver government services on-line. In fact, Canada has been remarkably successful. According to an annual survey of international government performance, by Accenture, a management consulting and technology services company, Canada ranked number one out of 22 countries for the fifth year in a row. Serving Canadians on-line is a government priority that promises less redundancy of information and better service to citizens.

However, the demands of e-government threaten the end of information silos which provide their own structural protection. Data silos may be antithetical to the concept of Government on-line or e-governments; there is no doubt that they are "less efficient". They duplicate information, and you can't get from one to another.

In contrast, government on-line may demand interoperable systems that pool personal information and make it available to more users for more purposes. The greater the amount of information, access, and number of users, the greater the vulnerability of the individuals to excessive government or bureaucratic surveillance.

Can we accept what amounts to a comprehensive personal file and still trust government not to misuse it—and, if so, how?

E-government may provide the critical push needed to make the *Privacy Act* a much more effective privacy framework. The Act must set out more stringent controls on access to the information pool. A better Act would also require greater justification for collecting information in the first place, one that needs to be clearly articulated. And a better Act would also demand a far stricter adherence to the principle that personal information be used only for the purposes for which it was collected.

E-government is upon us but the law is a long way behind. If government wants to become “the most connected to its citizens”, it must also be more protective of its citizens.

Extending the Scope of the *Privacy Act*

More than age enfeebles the *Privacy Act*. Perhaps most critical is the law’s function as a data protection statute, not a true privacy law. While not toothless, the best the law can manage in some circumstances is to “gum vigorously”. The Act essentially is a set of checks and balances on government power. It establishes a set of “fair information practices” to regulate federal government collection, use and disclosure of individuals’ personal data. And the law gives individuals the right of access to that information.

Expanding jurisdiction

As it is, there are gaps in the *Privacy Act*’s coverage: many institutions, including our own Office, are not subject to privacy law. Over the years, the federal government has created many entities that do not appear subject to either the *Privacy Act* or *PIPEDA*; they fall between the chairs. Such entities take the form of boards, tribunals, commissions, foundations, institutions, and corporations. They may operate as partnerships or joint ventures receiving funds from both the federal government and provincial governments. In our view, such a situation significantly weakens Parliament’s control with regard to the protection of personal information. Starting in the next fiscal year, we have undertaken an audit to determine and confirm the full extent of the gap and to assess risks in more detail. So far, we count over 30 entities not clearly subject to privacy legislation.

And as government creates new institutions, a debate ensues on adding (or not) the new body to the schedule of those covered. Arguably, the process is clumsy and the right sufficiently vital in a democracy to warrant giving the *Privacy Act* primacy over any other Act of Parliament. Thus the law would apply to all federal institutions unless the enabling or other departmental legislation expressly declares that it applies notwithstanding the *Privacy Act*. A similar provision already appears in *PIPEDA*.

Protecting unrecorded information

Technology has effectively demonstrated that limiting the *Privacy Act*’s application to personal information “recorded in any form” is well past its “best before” date.

The restrictive definition puts unrecorded information, such as from real-time electronic monitoring (live surveillance cameras) or from biological samples, beyond

the scope of the Act. Yet the technologies can yield intelligible information about identifiable individuals which should benefit from legal protection.

The proposal is workable; some provincial privacy laws and *PIPEDA* both apply to unrecorded information. For example, a security company in Northwest Territories and Nunavut mounted four security cameras on the roof of its building aimed at a main intersection in Yellowknife. For several days, 24 hours a day, staff monitored a live feed and reported a number of incidents to local police. The monitoring was intended to demonstrate the service and generate business for the company.

Although a public outcry quickly ended the demonstration, the Commissioner had the power to investigate and issue findings under *PIPEDA* which provides helpful guidance for other institutions. The Commissioner concluded that while monitoring public places may be appropriate for public safety reasons, there must be a demonstrable need, it must be done by lawful public authorities and done in ways that incorporate all legal privacy safeguards.

Extending access rights

Going global also means that Canadian government institutions now hold personal information about foreign nationals. For example, the CBSA collects Advance Passenger Information/Passenger Name Record of travellers entering Canada. The information includes name, date of birth, citizenship, passport or travel document number, reservation data and the traveller's itinerary. Airlines gather the information from passengers at the point of departure and send it to CBSA ahead of flight arrival.

However, under the *Privacy Act* only those present in Canada have the right to seek access to their personal information. This means overseas airline passengers, as well as immigration applicants, foreign student applicants, and countless other foreigners with information in Canadian government files, have no legal right to examine the information, to know how it is used or disclosed, or to complain to the Privacy Commissioner.

It is becoming increasingly difficult to justify hedging access rights in the face of international mobility and the ensuing exchange of personal data. Nor, in fact, does it appear balanced when other countries grant access rights to Canadians. For example, the European directive on privacy rights (with which 25 member states comply) grants access rights to “every data subject”—anyone whose information is held by a European entity.

The CBSA's collection of passenger information highlighted both the *Privacy Act's* shortcomings and the difficulties of ensuring even-handed treatment of the information. Although the CBSA has agreed "to administratively extend these rights to citizens who are not present in Canada", both the European Union's Working Group and the Privacy Commissioner would prefer that the law grant access to anyone.

Controlling data matching—effectively

Although government use of data matching (or "computer-matching") arguably poses the greatest threat to individuals' privacy, the *Privacy Act* is silent on the practice. Privacy Commissioners (bolstered by Parliamentary Committees) have all recognized the dangers inherent in excessive and unrelated data collection. All have recommended amending the *Privacy Act* to ensure that government institutions link personal records in discrete systems only when demonstrably necessary, and under the continued vigilant oversight of the Privacy Commissioner of Canada. The recommendations have not been followed through.

Granted not all improvements to the Act require legislative changes; administrative or policy directives often can fill the bill. But the Treasury Board issued guidelines in 1989 outlining the steps departments should take before matching data, including submitting a detailed proposal for the Privacy Commissioner's review. Given how few data matching proposals the Office of the Privacy Commissioner has received—and the likely extent of the practice—it is time to set out the obligations in law.

Limiting collection

Limiting collection is a fundamental principle of all data protection statutes. The *Privacy Act* requires government institutions to collect only personal information that is "directly related to" an operating program or activity authorized by Parliament. This gives government latitude to design programs with a defined set of personal information in mind. A more rigorous test would require institutions to demonstrate that the information is *necessary* for the program or activity.

Although the Treasury Board interprets the *Privacy Act* in this manner, Parliament should amend the law to put the matter beyond interpretation.

Government Transparency

The *Privacy Act* requires government institutions to inform individuals of the reason for collecting personal information. However, this response does not truly respect individuals' rights to control the collection, use and disclosure of their information.

A more meaningful explanation, and one more in keeping with modern data protection principles, should specify:

- a) the authority under which the information is being collected;
- b) the uses to which the information may be put;
- c) the institutions with which the information may be shared;
- d) whether the information is discretionary or mandatory;
- e) the consequences of not providing the information; and
- f) the individual's right to complain under the *Privacy Act*.

"Publicly available"

One exception to the *Privacy Act's* use and disclosure provisions is material that is "publicly available". This includes, for example, information available in public archives, libraries and museums. However, it also includes information contained in such public registries as the Bankruptcy Registry and the Lobbyist Registry. While there are good reasons for making these collections open to the public—transparency and accountability—few if any of the registries control the details they disclose or any subsequent uses made of the information. This has led to such abuses as bulk disclosures of personal information from the registries for marketing purposes.

Parliament should amend the *Privacy Act* to permit disclosures of personal information from these registries only in ways and for purposes consistent with the original purpose for establishing the registry.

Re-tooling the disclosure provisions

Perhaps the most evident demonstration of the weakness of the current *Privacy Act* in dealing with disclosures of personal information was provided by the Federal Court of Appeal in 2000 in the E-311 case (*Privacy Commissioner v. Attorney General of Canada*). The Court concluded that the disclosure provision in section 8(2)(b) of the *Privacy Act* enables Parliament to confer on any Minister (through a given statute) wide discretion to disclose information collected by the Minister's department.

The Privacy Commissioner argued that the *Privacy Act* required that the Minister disclose personal information only for the purpose for which it was collected, or for a use consistent with that purpose. However, the Court of Appeal found that section 8(2)(b) of the Act did not impose any such limitation. The Supreme Court "agreed substantially" the following year.

The *Privacy Act* also sets out in subsection 8(2) specific circumstances in which government institutions may disclose personal information without the individual's consent. Among these are disclosures to named investigative bodies, to Public Archives, to MPs to help constituents, to provincial and foreign governments, and for research and statistical purposes.

Some of these disclosures seem too permissive; for example, section 8(2)(f) authorizes disclosures under an agreement or arrangement between the Government of Canada and the government of a province or a foreign state. This provision needs to be much more specific as to the parameters of any such sharing and provide guidance on the kinds of contract provisions that are needed to safeguard privacy.

When Canadians share their information with the Canadian government at home or in consulates abroad, they do so with the expectation that this information will not generally make its way into the hands of foreign states. The current wording of section 8(2)(f) is broad and leaves much discretion to departments. There should be an obligation to thoroughly examine why the information is required by the foreign state, how it will be used, on what authority the request is made, and whether there are adequate safeguards to protect the information, including provisions protecting against secondary release. Pending reform of the *Privacy Act*, the Privacy Commissioner is actively encouraging government institutions to self-impose higher standards.

After more than 20 years overseeing the *Privacy Act's* administration, it is evident to us that the disclosure provisions need review and substantial revision.

Enabling the Privacy Commissioner

Moving from the pure "ombudsman" role

The *Privacy Act* gives the Privacy Commissioner of Canada the powers of an ombudsman, with no inherent powers of enforcement. The Privacy Commissioner can, however, go to Federal Court in certain circumstances. While the ombudsman model has been an effective one in avoiding an adversarial climate to encourage compliance, appeals to fairness and good sense are only as effective as the compliance they engender.

Models in several other jurisdictions, both in Canada and abroad, give the overseer the tools to compel respect for the law. Parliament may wish to review the merits of such powers for the Privacy Commissioner of Canada.

Conducting research and public education

For years, succeeding Privacy Commissioners have argued that the burgeoning threats to Canadians' privacy warrant an informed and effective voice for privacy. The Commissioner's Office needs both the power and the resources to conduct research and prepare reports on privacy issues, educate the public about their privacy rights, and evaluate the privacy implications of proposed legislation.

While Parliament heard the pleas during drafting of *PIPEDA*—and how valuable the tools have proven to be—the Commissioner has not been given the same mandate for public education under to the *Privacy Act*. The Commissioner should be equally empowered to sensitize business, government and the public under both laws.

Strengthening Court Review

Finally, complainants—and the Privacy Commissioner—may only seek a Court review of, and remedies for, denials of access to their personal information. Effectively this means that allegations of improper collection, use and disclosure may not be challenged before the Court, and the subsequent benefit of the Court's guidance on all government institutions is lost. Nor does the *Privacy Act* contemplate remedies for any damages caused by government actions.

Even when the Commissioner agrees that the complaint has merit, the Federal Court decided in March 2005 (in *Murdoch v. Canada (Royal Canadian Mounted Police)*) that neither the Court nor the Privacy Commissioner has any powers beyond those set out in the *Privacy Act*.

Individuals, or the Commissioner acting on their behalf, should be able to ask the Court to review government collection, use and disclosure of personal information. As well, the Commissioner, in his or her capacity as complainant, should be allowed to apply to the Court for review of any matter to which the *Privacy Act* applies. And the Court should be empowered to assess damages against offending institutions.

Privacy Management Framework

Building a Privacy Management Framework for the Federal Government

What is a framework?

Generally management frameworks serve as blueprints to help an institution achieve a desired result. They establish goals and policies, and describe the systems, procedures and performance measurements needed to meet those goals. Properly constructed and applied, frameworks can be powerful instruments for showing institutions how best to conduct an activity, and how to marshal and allocate resources to achieve results.

While the concept is not new in management circles, applying it in the privacy context is. A government-wide model privacy management framework should be designed to help departments protect the personal information they control by identifying the inherent privacy risks, and how best to mitigate those risks.

OPC interest in privacy management frameworks

Our Office continually seeks improvements in the federal government's privacy management. We do so assuming that:

- The *Privacy Act*, (despite needed reform), should not inhibit improved privacy management;
- Improvements can be achieved through policy and guidelines; and

- Treasury Board Secretariat (TBS), as the locus for privacy policy, should ensure that federal departments and agencies meet high privacy management standards.

For example, in August 2004 our Office submitted a brief to the government on the implications of the *USA PATRIOT Act*. We suggested the federal government examine the circumstances under which it allows Canadians' personal information to be processed outside of Canada—and thus beyond the protection of the *Privacy Act*.

The Privacy Commissioner subsequently wrote to the President of Treasury Board requesting his support on this matter.

In response, TBS began reviewing the federal government's arrangements for outsourcing personal information. It also began developing model contractual clauses that departments could use to reduce the potential privacy risks to personal information being processed by U.S. companies or U.S. affiliates subject to the *USA PATRIOT Act*. This work is critically important and TBS expects to complete it shortly.

Our Office also suggested TBS review the federal government's data mining and assembly, re-examine the dated (1989) data matching policy, and strengthen the reporting requirements under the *Privacy Act*. These are also underway. We applaud the initiatives, as well as new privacy reporting requirements TBS issued in April 2005.

On the face of it the reporting guidelines indicate a desire for stronger privacy management. After new guidelines have had a chance to work, our Office intends on examining privacy reporting in some depth to determine which annual reports and statistical data are most effective in explaining privacy activity and issues, and supporting sound privacy management.

While each of these initiatives is significant, collectively they highlight the need for a more comprehensive and consistent approach to managing privacy in the federal government. A privacy management framework would help achieve this goal.

What makes a good privacy management framework?

First, TBS and departments—not our Office—are responsible for ensuring that an appropriate privacy management framework is in place. The design and implementation of frameworks need to be driven from within, not imposed externally. An external oversight body such as our Office certainly can, and should,

suggest the key attributes of an effective framework. We can also review and audit after the fact to determine whether a framework is working as intended. However, departmental ownership of the process is critical to its success.

The idea of privacy management frameworks appears to be gaining momentum in the federal government. The Assistant Deputy Minister Privacy Committee (chaired by TBS, the department of Justice and the Privy Council Office) has met periodically to promote a coherent and effective federal approach to privacy which includes developing an overall privacy framework and the sharing of best practices.

Some departments are already at work. For example, Human Resources and Skills Development Canada (HRSDC) presented their privacy management framework to the ADM Privacy Committee in June 2004. The department is a heavy user of personal data since it administers (among others) the Employment Insurance and Canada Student Loan programs. The framework aims to build trust with citizens by giving them more information about departmental programs and how they use and disclose individuals' personal information.

HRSDC defines the four pillars of their privacy management framework as:

- **strategic planning and governance**—conducting research and analysis to better understand citizens expectations on privacy, and defining the core privacy principles for their operations;
- **risk management**—establishing a review and approval protocol for privacy impact assessments, setting standards for personal information-sharing agreements and carrying out privacy reviews of research databases;
- **cultural change**—providing training for all managers, staff and contractors on personal information management, including specialized training on the requirements of specific programs; and
- **assuring compliance**—developing internal audit standards for managing personal information.

HRSDC found that adopting a privacy management framework provided the department a renewed impetus for improving their personal information management. The framework established a common platform both for defining better privacy practices, and helping it take the initiative in identifying and resolving issues. We applaud the department's leadership and commitment to fair information practices.

With a little help from Privacy Impact Assessments

Conducting privacy impact assessments (PIAs) provides another impetus for developing sound privacy management frameworks. Since May 2002, Treasury Board policy requires federal departments and agencies to conduct PIAs for all new programs or services that raise potential privacy issues. The assessments are designed to forecast potential privacy problems and identify options to mitigate risks before beginning a project.

The PIA policy is not only a key component of any good privacy management strategy; the policy itself promotes adopting a structure that is essentially a privacy management framework. The PIA policy guidelines, for example, require department heads to define the roles of their personnel in adhering to the requirements. Department heads must also assume responsibility for overseeing implementation—accountabilities that lie at the core of a privacy management framework. The policy also serves as an instrument for both promoting awareness of sound privacy practices, and measuring a department's compliance with privacy best practices.

The Treasury Board would be responsible for promulgating a model privacy management framework. A flexible approach should be taken in designing and applying a model. We recommend it possess the following attributes:

- Communicates effectively the importance of personal information management and the commitment to building privacy into program management;
- Sets clear objectives and standards on personal information gathering, quality, use, security, transmission, access, disclosure, retention and disposal;
- Clarifies the roles and responsibilities, and provides a basis for determining the resources and skills needed for achieving sound privacy management;
- Relies on sound risk management approaches, particularly through privacy impact assessments and/or threat risk assessments;
- Uses effective controls to support compliance and best practices—integrating best available privacy-enhancing technology, resolving disputes effectively, and identifying and correcting system weakness or privacy incidents; and
- Promotes accountability and continuous improvement through such means as reporting, audit and evaluation, education, and performance appraisals.

Since the concept is new, inevitably there will be some fine tuning—driven by experience and experimentation. In fact we are in the midst of a major audit that will allow us to test, refine and validate our approach. Once completed, we expect the audit will further substantiate the value of a privacy management framework.

Privacy is, in many respects, a risk management issue. Privacy management frameworks are of vital importance in helping federal institutions manage that risk. Accordingly, we recommend that the TBS develop a model framework to guide privacy management in federal departments and agencies.

We have discussed our recommendation for a model framework with TBS management. The President of the Treasury Board is committed to exploring the concept of a government-wide privacy management framework. We understand that TBS has begun examining both the scope and process for a project that should build on existing management frameworks. The project will require dedicated resources, cooperation among stakeholders (including our Office), effective communication with departments, and appropriate compliance mechanisms.

We welcome the initiative.

Complaints

Introduction

The *Privacy Act* has been in force since 1983, protecting individuals' personal information held by federal government departments and agencies. The Act governs those institutions' collection, use, disclosure, retention and disposal of the personal information they hold to administer government programs. Individuals also have the right to request access to and correction of their government-held personal information. The Act also sets out the duties, responsibilities and mandate of the Privacy Commissioner of Canada.

The Commissioner receives and investigates complaints from individuals who believe their *Privacy Act* rights have been violated. The Commissioner may initiate a complaint and investigate any situation where she has reasonable grounds to believe the Act has been violated.

The Privacy Commissioner of Canada is an ombudsman who resolves complaints through mediation, negotiation, and persuasion whenever possible. However, the Act gives the Commissioner broad investigative powers to carry out her mandate. She may subpoena witnesses, compel testimony, and enter premises to obtain documents or to conduct interviews. It is an offence under the Act to obstruct an investigation.

The Act does not grant the Commissioner order-making powers. Nevertheless, the Commissioner can and does recommend necessary changes to the information-handling practices of government institutions. The Commissioner may audit any federal department or agency at any time, and may recommend changes to any practices that are not in compliance with the *Privacy Act*.

The Commissioner is required to submit an Annual Report to Parliament, detailing the activities of the Office in the previous fiscal year. This report covers the period from April 1, 2004 to March 31, 2005 for the *Privacy Act*.

Investigations and Inquiries

Complaints Received

The Office received 1,577 complaints under the *Privacy Act* in 2004-05, down from 4,206 in 2003-04. While this is a significant decrease, the 2003-04 volume was an all-time high due to specific circumstances: almost 500 aboriginal Canadians filed complaints against a Health Canada consent form; and correctional officers, staff and inmates filed more than 2000 complaints against Correctional Service Canada. This year's volume is a return to a more normal year.

Definitions of Complaint Types

Complaints received in the Office are categorized into three main groups:

Access:

- **Access.** All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.
- **Correction/Notation.** The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.
- **Language.** Personal information was not provided in the official language of choice.
- **Fee.** Fees have been assessed to file a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.
- **Index.** INFOSOURCE¹ does not adequately describe the personal information holdings of an institution.

¹ INFOSOURCE is a federal government directory that describes each institution and the banks of information (group of files on the same subject) held by that particular institution.

Privacy:

- **Collection.** Personal information collected that is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.
- **Retention and Disposal.** Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in INFOSOURCE¹): either destroyed too soon or kept too long.

In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.

- **Use and Disclosure.** Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible disclosures without consent listed in section 8(2) of the Act.

Time Limits:

- **Time Limits.** The institution did not respond within the statutory limits.
- **Extension Notice.** The institution did not provide an appropriate rationale for an extension, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.
- **Correction/Notation Time Limit.** The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

COMPLAINTS RECEIVED BY COMPLAINT TYPE

Received between April 1, 2004 and March 31, 2005

This table shows the number of complaints received by Complaint Type.

Complaint Type	Total	Percentage
Access	604	38%
Correction-Notation	29	2%
Language	2	0%
Collection	92	6%
Retention and Disposal	17	1%
Use and Disclosure	250	16%
Time Limits	489	31%
Extension Notice	90	6%
Correction-Time Limits	4	0%
Total	1,577	100%

TOP TEN DEPARTMENTS BY COMPLAINTS RECEIVED

Year ending March 31, 2005

This table represents the departments that received the greatest number of complaints in the reporting period.

It should be noted that this does not necessarily mean that these departments are exercising poor compliance with the *Privacy Act*. Rather, some of these departments because of their mandate hold a substantial amount of personal information about individuals and are therefore more likely to receive numerous requests for access to that information. A large amount of personal information increases the likelihood of complaints about the department's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

Institution	Total	Access	Time	Privacy
Correctional Service of Canada	395	162	84	149
Immigration and Refugee Board	222	96	126	0
Canada Revenue Agency	183	69	64	50
Royal Canadian Mounted Police	155	58	67	30
Citizenship and Immigration Canada	118	39	72	7
National Defence	72	25	34	13
Canada Post Corporation	60	32	1	27
Canadian Security Intelligence Service	49	46	2	1
National Research Council Canada	47	0	46	1
Justice Canada	32	14	17	1
Others	244	94	70	80
Total	1,577	635	583	359

COMPLAINTS RECEIVED BY RESPONDENT

Received between April 1, 2004 and March 31, 2005

This table shows the actual number of all of the complaints lodged against the various departments and agencies that were received in the reporting period.

Institution	Total
Agriculture and Agri-Food Canada	2
Atlantic Canada Opportunities Agency	1
Bank of Canada	1
Canada Border Services Agency	26
Canada Customs and Revenue Agency	6
Canada Post Corporation	60
Canada Revenue Agency	183
Canada School for Public Service	1
Canadian Firearms Centre	1
Canadian Food Inspection Agency	2
Canadian Human Rights Commission	3
Canadian Nuclear Safety Commission	1
Canadian Security Intelligence Service	49
Citizenship and Immigration Canada	118
Commission for Public Complaints Against the RCMP	3
Correctional Investigator Canada	2
Correctional Service Canada *	395
Elections Canada	1
Environment Canada	4
Farm Credit Canada	1
Financial Transactions and Reports Analysis Centre of Canada	1
Fisheries and Oceans	8
Foreign Affairs and International Trade Canada	24
Health Canada	27
Human Resources and Skills Development Canada	41
Immigration and Refugee Board **	222
Indian and Northern Affairs Canada	4
Industry Canada	3
Justice Canada, Department of	32
Military Police Complaints Commission	1
National Archives of Canada	3
National Capital Commission	5
National Defence	72
National Gallery of Canada	2
National Parole Board	10
National Research Council Canada	47

* CSC - A large portion of these complaints were submitted by Correctional Officers in the course of their labour relations negotiations with their employer.

** IRB - A significant portion of these complaints were submitted by one individual in the course of dealing with the IRB.

COMPLAINTS RECEIVED BY RESPONDENT (cont.)

Received between April 1, 2004 and March 31, 2005

This table shows the actual number of all of the complaints lodged against the various departments and agencies that were received in the reporting period.

Natural Resources Canada	8
Natural Sciences and Engineering Research Council of Canada	1
Office of the Chief Electoral Officer	11
Privy Council Office	1
Public Service Commission Canada	6
Public Service Human Resources Management Agency of Canada	1
Public Service Staff Relations Board	1
Public Works and Government Services Canada	3
Royal Canadian Mounted Police ***	155
Social Development Canada	18
Statistics Canada	1
Transport Canada	1
Veterans Affairs Canada	5
Western Economic Diversification Canada, Department of	3
Total	1,577

*** RCMP - A great number of these complaints are time related complaints since the RCMP was not able to respond to requests within the legislated time frames imposed by the *Act*.

Complaints Completed

We closed 2,407 complaints under the *Privacy Act*, over 800 more than our Office received in the year. However, almost 1,000 of those complaints were from one group of individuals—correctional officers requesting copies of their employee personnel files. Since many were similar, they required less work than would 1,000 unique complaints (once one complaint is concluded, the documentation serves as a model for many others). Nevertheless, the investigators accomplished a formidable task in closing so many cases, particularly since there were fewer staff than in previous years and investigators were diverted on a rotational basis to help the Inquiries Unit.

Despite closing more *Privacy Act* complaints than it received, the Office is carrying a significant number of ongoing cases—1,277 at fiscal year end. Resource levels were not sufficient to keep up with demand. Year end saw the final stages of a major Business Process Review of the Investigations and Inquiries Branch which was undertaken to streamline processes wherever possible, help establish appropriate resource levels, and solve our ever-growing aging caseloads.

Normally we would expect to close approximately 1,185 complaints with the allocated staff. With an annual intake in excess of 1,500, we are losing ground; the caseload is aging and by fiscal year-end 577 complaints remained unassigned due to lack of staff. We have limited open caseloads to 35 per investigator at a time. Some of the unassigned cases are now nearly a year old. Even older complaints being actively investigated take more time as the delay becomes a factor in finding documents and dealing with fading memories. The Branch's established standard of investigators completing 75 cases each year means that it would take approximately eight investigators one year to clear the unassigned cases alone.

Definitions of Findings under the *Privacy Act*

The Office has developed a series of definitions of findings to explain the outcome of its investigations under the *Privacy Act*.

Not Well-founded: the investigation uncovered no or insufficient evidence to conclude that the government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: the government institution failed to respect the *Privacy Act* rights of an individual.

Well-founded/Resolved: the investigation substantiated the allegations and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: after a thorough investigation, the Office helped negotiate a solution that satisfies all parties. The finding is used for those complaints in which "well-founded" would be too harsh to fit what essentially is a miscommunication or misunderstanding.

Settled during the course of the investigation: the Office helped negotiate a solution that satisfies all parties during the investigation, but issues no finding.

Discontinued: the investigation was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons—the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Early resolution: applied to situations in which the issue is dealt with before a formal investigation is undertaken. For example, if an individual complains about an issue that the Office has already investigated and found to be compliant with the *Privacy*

Act, we explain this to the individual. We also receive complaints in which a formal investigation could have adverse implications for the individual. We discuss the possible impact at length with the individual and should he or she choose not to proceed further, the file is closed as "early resolution". This is a new type of disposition which the Office began using in April 2004.

COMPLAINT FINDINGS BY COMPLAINT TYPE

Closed between April 1, 2004 and March 31, 2005

This table clearly shows the total number of the various findings issued by the Office by complaint type in the reporting period.

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled during investigation	Well-founded	Well-founded-Resolved	Total	Percentage
Access	44	22	1,170*	18	120	21	21	1,416	59%
Correction-Notation	1	0	5	0	3	0	0	9	0%
Language	1	0	0	1	0	0	0	2	0%
Collection	3	11	32	2	12	6	0	66	3%
Retention & Disposal	0	2	7	0	2	2	1	14	1%
Use & Disclosure	29	43	143	1	63	138	1	418	17%
Time Limits	15	9	42	0	5	361**	0	432	18%
Extension	1	0	14	0	0	23	0	38	2%
Notice									
Correction-Time Limits	1	0	0	0	0	11	0	12	0%
Total (# and %)	95 (4%)	87 (4%)	1,413 (59%)	22 (1%)	205 (8%)	562 (23%)	23 (1%)	2,407	100%

* As mentioned previously a large portion of the complaints determined to be not well-founded were submitted by the Correctional Officers in CSC who invoked the access provisions of the Act and its subsequent complaints mechanism in the course of their on-going labour dispute with CSC. In these cases CSC had decided to provide the Correctional Officers with their personal information by using a particular method of access to which the Correctional Officers objected. Our subsequent investigation of these complaints determined that CSC had the authority to choose the method of access and that it was compliant with the *Privacy Act* in doing so.

** A large number of time limit complaints were lodged against some departments that are facing significant resourcing problems. While we can sympathize, the *Privacy Act* simply does not provide this Office with any flexibility about refusing to investigate these complaints. Departments and agencies are required to respond to each and every privacy request and our role is to see that departments properly apply the *Privacy Act*. Having said this we are aware that some institutions are addressing their resourcing issues and commend them for dealing with their problem. We look forward to seeing the impact that these new resources will have on the number of complaints and will report on this issue in the next annual report.

COMPLETED COMPLAINTS BY ORIGIN

Closed between April 1, 2004 and March 31, 2005

This table shows the province of origin of the complaints investigated in the reporting period. It is to be noted that some complaints were received from some persons living outside of Canada.

Province/Territory	Total
Quebec	1,090*
Ontario	641*
British Columbia	274
NCR (ON)	106
Alberta	81
New Brunswick	59
Saskatchewan	40
NCR (QC)	39
Manitoba	34
Nova Scotia	17
Prince Edward Island	6
International	6
Newfoundland and Labrador	5
Northwest Territories	3
Nunavut	3
Yukon Territory	3
Total	2,407

* A significant portion of both these figures is attributable to the complaints lodged by the Correctional Officers in CSC.

COMPLETED COMPLAINTS AND RESULTS BY RESPONDENT

Closed between April 1, 2004 and March 31, 2005

This table shows the number of completed complaints by respondent and by finding.

Respondent	Discontinued	Early Resolution	Not well founded	Resolved	Settled during investigation	Well-founded	Well-founded Resolved	Total
Agriculture & Agri-food Canada	0	0	2	0	1	0	0	3
Auditor General of Canada, Office of the	0	0	1	0	0	0	0	1
Business Development Bank of Canada	0	0	0	0	1	0	0	1
Canada Border Services Agency	0	7	0	0	0	2	0	9
Canada Customs & Revenue Agency	28	2	56	3	28	16	3	136
Canada Mortgage & Housing Corporation	0	0	0	0	0	0	1	1
Canada Post Corporation	5	9	29	0	12	37	3	95
Canada Revenue Agency	2	11	41	3	2	26	0	85
Canadian Firearms Centre	1	1	0	0	0	0	0	2
Canadian Food Inspection Agency	0	1	0	0	1	1	0	3
Canadian Heritage	0	0	1	0	0	0	0	1
Canadian Human Rights Commission	0	0	0	1	0	1	0	2
Canadian Museum of Civilization	0	1	0	0	0	0	0	1
Canadian Security Intelligence Service	1	0	16	0	9	1	0	27
Canadian Space Agency	0	0	1	0	0	0	0	1
Canadian Tourism Commission	0	0	0	0	0	3	1	4
Citizenship & Immigration Canada	6	7	26	0	22	52	2	115
Commission for Public Complaints Against the RCMP	0	0	1	0	0	2	0	3
Correctional Investigator Canada	0	0	2	0	0	1	1	4
Correctional Service Canada	12	20	1,112 *	5	54	305	2	1,510
EDULINX Canada Corporation	0	1	0	0	0	0	0	1
Environment Canada	0	0	1	0	0	0	0	1
Finance Canada, Department of	0	0	0	0	0	0	1	1
Financial Transactions & Reports Analysis Centre of Canada	0	0	1	0	0	1	0	2
Fisheries & Oceans	0	0	4	0	0	0	1	5
Foreign Affairs & International Trade Canada	0	1	5	0	3	9	0	18
Health Canada	1	0	2	1	2	6	1	13

* This figure clearly shows that CSC had appropriately responded to the large number of access requests it had received from its Correctional Officers and that it was compliant with the requirements of the Act.

COMPLETED COMPLAINTS AND RESULTS BY RESPONDENT (cont.)

Closed between April 1, 2004 and March 31, 2005

This table shows the number of completed complaints by respondent and by finding.

Respondent	Discontinued	Early Resolution	Not well founded	Resolved	Settled during investigation	Well-founded	Well-founded Resolved	Total
Human Resources & Skills Development Canada	12	9	26	1	8	6	3	65
Immigration & Refugee Board	0	0	4	0	6	2	0	12
Indian & Northern Affairs Canada	0	1	0	0	5	0	0	6
Industry Canada	0	0	1	1	1	0	0	3
Justice Canada, Department of	1	2	3	1	3	7	0	17
National Archives of Canada	0	0	2	0	0	0	0	2
National Capital Commission	0	1	0	0	0	0	0	1
National Defence	5	4	10	4	15	33	0	71
National Gallery of Canada	0	0	0	0	1	0	0	1
National Parole Board	1	0	15	0	1	1	0	18
National Research Council Canada	0	0	0	0	1	0	0	1
Ombudsman National Defence & Canadian Forces	0	0	0	0	0	0	1	1
Pension Appeals Board Canada	0	0	0	0	1	0	0	1
Privy Council Office	0	0	0	0	0	1	0	1
Public Service Commission Canada	0	1	3	0	0	0	0	4
Public Works & Government Services Canada	0	0	2	0	4	0	1	7
Royal Canadian Mint	0	0	1	0	0	0	0	1
Royal Canadian Mounted Police	15	5	33	1	19	43	1	117
Social Development Canada	0	0	1	0	3	2	0	6
Solicitor General Canada	0	0	0	0	0	2	0	2
Statistics Canada	1	1	2	0	0	0	0	4
Status of Women Canada	0	0	2	0	0	0	0	2
Transport Canada	0	1	4	1	2	2	1	11
Veterans Affairs Canada	1	1	3	0	0	0	0	5
Western Economic Diversification Canada, Department of	3	0	0	0	0	0	0	3
Total	95	87	1,413	22	205	562	23	2,407

Investigation Process under the *Privacy Act*

Inquiry:

Individual contacts OPC by letter, by telephone, or in person to complain of violation of the Act. Individuals who make contact in person or by telephone must subsequently submit their allegations in writing.



Initial analysis:

Inquiries staff review the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act.

An individual may complain about any matter specified in section 29 of the *Privacy Act* – for example, denial of access, or unacceptable delay in providing access, to his or her personal information held by an institution; improper collection, use or disclosure of personal information; or inaccuracies in personal information used or disclosed by an institution.



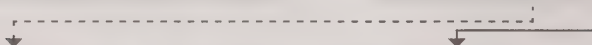
Complaint?

No:

The individual is advised, for example, that the matter is not in our jurisdiction.

Yes:

An investigator is assigned to the case.



Early resolution?

A complaint may be resolved before an investigation is undertaken if, for example, the issue has already been fully dealt with in another complaint and the institution has ceased the practice.

Investigation:

The investigation will serve to establish whether individuals' privacy rights have been contravened or whether individuals have been given their right of access to their personal information.

The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner or her delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

Discontinued?

A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.

Analysis (on next page)

Settled? (on next page)

Analysis:

The investigator analyzes the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Branches, as appropriate.

Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the institution are warranted.

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the institution. The Privacy Commissioner or her delegate may ask the institution to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.

The possible findings are:

Not Well-Founded: The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the *Act* have been contravened.

Well-Founded: The institution failed to respect a provision of the *Act*.

Well-Founded, Resolved: The investigation substantiated the allegations and the institution has agreed to take corrective measures to rectify the problem.

Resolved: The evidence gathered in the investigation supports the allegations raised in the complaint, but the institution agreed to take corrective measures to rectify the problem, to the satisfaction of this Office. The finding is used for those complaints in which Well-Founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court on matters of denial of access to personal information.

Where recommendations have been made to an institution, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the denial of access. The Federal Court has the power to review the matter and determine whether the institution must provide the information to the requester.

Settled?

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through negotiation and persuasion. The investigator assists in this process.

Note: a broken line (- - -) indicates a *possible* outcome.

COMPLAINT INVESTIGATIONS TREATMENT TIMES - *PRIVACY ACT*

This table represents the average number of months it has taken to complete a complaint investigation by disposition, from the date the complaint is received to when a finding is made.

By Disposition

For the period between April 1, 2004 and March 31, 2005.

Disposition	Average Treatment Time in Months
Early Resolution	2.2
Well-Founded	6.1
Not Well-Founded	6.1
Discontinued	6.7
Settled in the Course of Investigation	10.1
Well-Founded, Resolved	11.5
Resolved	12.0
Overall Average	6.4

By Complaint Type

For the period between April 1, 2004 and March 31, 2005.

This table represents the average number of months it has taken to complete a complaint investigation by complaint type, from the date the complaint is received to when a finding is made.

Complaint Type	Average Treatment Time in Months
Correction/Notation Time Limit	4.1
Extension Notice	4.4
Time Limits	5.6
Access	6.3
Use and Disclosure	7.2
Collection	9.4
Retention and Disposal	10.0
Correction/Notation	10.7
Overall Average	6.4

Upon reviewing this table, one can see that the less complex complaints (Time Limits and Extension Notice) were completed in a shorter period of time than the more complex ones. This is reasonable since the more complex complaints usually require more on-site interviews, more in-depth research and analysis and, often times, lengthier negotiations with an institution regarding proposed corrective measures when there has been a breach of the Act.

Follow-up after Investigations

Once a complaint is investigated and completed, the story does not necessarily end there. All complaints dealing with improper collection, use, disclosure and retention that are well-founded are sent to the Audit and Review Branch for its review. This allows the Branch to identify any trends and patterns dealing with privacy breaches and use this information in planning and developing its audits for the next year.

Select cases under the *Privacy Act*

The cases described below have been selected for their educational value. They demonstrate the importance of correctly handling personal information and what can go wrong if this does not occur. It is hoped that they will encourage government institutions and agencies to be ever vigilant in handling personal information in accordance with the Act and to engage in ongoing staff education in that regard. At the same time, members of the general public may be prompted to ask questions about how their personal information is being handled by federal institutions and know that they can complain to this Office should something go wrong.

Outside psychologist's notes still "under control of" RCMP

An RCMP member, under investigation for allegedly uttering threats and unlawful use of a firearm, complained that the force denied her access to information gathered during its investigation. She did not receive a copy of a videotaped interview or the notes and psychometric data from interviews with a psychologist.

The privacy investigator determined that some of the information she sought in the videotaped interview with an RCMP investigator contained information about other people—an exemption under the *Privacy Act*. The force was able to remove these segments and provide her with the remaining information.

More problematic were the psychologist's records. The RCMP did not have copies of the material since the services were provided, not by a staff member, but by an outside professional on a fee for service basis. Pressed by the investigator, RCMP staff obtained some of the information but the psychologist refused to provide the psychometric data and what he termed his "personal notes" unless served with a court order. He argued that disclosing the material would breach his profession's ethical standards.

The RCMP's attempts at persuasion yielded nothing until the OPC wrote formally to the former Commissioner advising him that since the RCMP had hired the psychologist to assess the member, all the information prepared or created for the assessment was "under the control of" the RCMP for *Privacy Act* purposes. The psychologist eventually provided his notes, as well as the psychometric data which the RCMP sent to the complainant's doctor for explanation and interpretation.

Our Office concluded that the complainant eventually received the appropriate information but her complaint was well-founded. We reminded the RCMP that personal information collected on its behalf by outside experts is still under its control and thus subject to individuals' access. Contracts should make this clear.

Tax information disclosure narrower than it appears

A man complained that he was being forced to provide his province's drug insurance program with his income tax information before receiving the benefits.

This is a provincial drug insurance program providing financial assistance to residents who need help paying for prescription drugs. The program's level of assistance is tied to the family's net income—the less you earn, the more help you receive. Not surprisingly, the program verifies applicants' income by seeking their consent for the Canada Revenue Agency (CRA) to release their income information to the insurance program.

However, the consent form is very broad and appears to allow the program to see virtually all an individual's tax return. The privacy investigator followed up with CRA's Federal and Provincial Affairs Division. Staff explained that the breadth of the consent was dictated by the wording contained in the Memorandum of Understanding (MOU) with Ministry of Health. The key words in the consent form are "relevant to and solely for the purpose of determining, verifying and administering my level of benefit..."

To determine just what information meets those criteria, the privacy investigator examined the MOU and confirmed that CRA provides only three income amounts to the program: lines 236—Net Income; 303—Married Amount, and 5105—Net Income of Spouse as Reported Under GST Credit.

The complainant was satisfied with the investigator's findings and appreciative of the Office's efforts to determine how the program worked. He did not need any further action and the complaint was considered settled in the course of investigation.

Offender given caregiver's personal information

A woman complained that Correctional Service Canada (CSC) gave extensive personal information about her to an offender for whom she was caring.

The woman provides palliative care in her home to the elderly and those with special needs. CSC assessed the complainant to determine whether the home would be an appropriate facility in which to place offenders with special needs. CSC visited her home, conducted a full interview, prepared a Private Home Placement Report and approved the facility. The individual subsequently agreed to take in an offender whom the National Parole Board (NPB) had granted day parole. The offender needed placement in a facility capable of handling his extensive physical and mental conditions while also meeting the conditions of his parole. CSC considered him an unrepentant child molester and at danger of re-offending.

Once the offender was approved to move into the woman's care, he wrote to her saying that he had seen "your report from NPB" and that he understood her problems. The day after he moved into her home, he produced his address book in which he had written the names and telephone numbers of two of the woman's references to CSC. He also produced an entire copy of the Private Home Placement Report – a document the woman had never seen. The report included information about the woman's family members including information about her childhood, her marital history and current status, and educational and employment history.

The complainant was shaken by the offender's revelations and got in touch with local CSC parole officials. They agreed to her removing the report from the offender's room and blacking out her references' names and telephone numbers from his address book.

The investigation revealed that CSC officials originally intended releasing the offender to another facility but had to change plans. They then had to seek the NPB's approval to change the release destination. The offender's particular situation and his required level of care prompted Parole Board members to ask for more information about the private home placement. CSC provided the Placement Report to the Parole Board; it was then given to the board members who subsequently approved the change of

destination. The investigator was satisfied that the offender had not disclosed the information to anyone else.

At issue was whether CSC contravened the *Privacy Act* by giving the report to the offender. The *Corrections and Conditional Release Act (CCRA)* requires the Parole Board to share with the offender the information it uses to reach a decision about him or her. However, the information can be in the form of a summary or the “gist” of the information. The CCRA also allows the Parole Board to withhold “as much information as strictly necessary” (Section 144(4)) if the disclosure could jeopardize someone’s safety, the security of a correctional institution, or the conduct of a lawful investigation.

It was evident from the investigation that only the Parole Board members who were deciding on the application had actually read the Placement Report. No-one else at the NPB had read the full report and so none knew the extent of the personal details it contained. The NPB contended that CSC was responsible for ensuring that information was lawfully shared with the offender. NPB officials were also adamant that the law’s requirements would have been fully met had CSC given the offender only the “gist” of the report. Unfortunately no one at CSC had read the report before giving it to the offender so they too were unaware of its contents.

The OPC found the case extremely disturbing, given the offender’s history, the nature of the information in the report, and the fact that he was residing in her home. We understood that NPB and CSC officials were under time constraints to place the offender as quickly as possible and there was no malicious motive for the disclosure. Nevertheless, we found it disconcerting that the woman’s personal information was disclosed simply because no one took the time to read the report. The disclosure should never have happened. The *Privacy Act* has been in force since 1983 and federal government employees are constantly reminded of their obligations to protect personal information.

Our Office concluded that CSC had seriously contravened the woman’s confidentiality rights and that the complaint was well-founded. Unfortunately the *Privacy Act* provides no remedies or grounds for court review in the case of an improper disclosure of personal information.

The case has led to an agreement that CSC will no longer provide Placement Reports to the NPB.

Expired passports insufficient identification—for a passport

A man trying to renew his passport to attend a conference in Sweden questioned:

- Why he had to provide additional identifying information;
- Why an expired passport was not sufficient identification even though it was provided by a competent federal authority; and
- In what circumstances the Passport Office could refuse a document issued by a competent federal authority.

The complainant was opposed to providing a health card, firearms permit or driver's licence as proof of identity, arguing that Canadians are under no legal obligation to hold any of these documents and requiring any of them was both a violation of the Charter and the *Privacy Act*. The man also objected to providing his employer's address or that of any educational institution he attended in the past two years since either requirement would effectively preclude retired or unemployed persons from obtaining a passport.

Finally the man claimed that the Passport Office's demand for at least two references from people other than family members made it difficult for those, like himself, whose ill health or physical disability limits their contacts. He also argued that family members should not be automatically excluded as references.

The privacy investigator met Passport Office staff to review the requirements. The power to issue a passport comes from exercising Royal Prerogative not a particular law. The Passport Office (a Special Operating Agency of the Department of Foreign Affairs and International Trade), collects the passport information under the authority of an Order in Council *Canadian Passport Order* which gives the Minister the power to prescribe which forms will be used before issuing the passport. A third page was added to the application following September 11, 2001 to satisfy the department's concerns that the process was secure. The third page asks for addresses during the preceding two years, as well as for references.

Since a passport establishes the identity and citizenship of the bearer abroad, its validity is heavily dependent on the accuracy of the applicant's statements. Confirming the information with references who have known the applicant for at least two years helps substantiate its accuracy. However, applicants who cannot provide such references can complete form *PPT 132-Declaration in lieu of guarantor* and may also be able to name a family member in some circumstances.

The Passport Office confirmed that it cannot accept either an expired passport or Canadian birth certificate as supplementary identification because both were issued under less rigorous rules and can be forged. The office now demands the additional information to support the accuracy of the applicant's statements, and help avoid circulation of false passports. Applicants can use expired passports as proof of Canadian citizenship but not as a secondary piece of identification.

Our Office concluded that the Passport Office has the legal authority to collect the additional information to confirm the applicant's identity. The intent is not to impose draconian restrictions on applicants but to give the Passport Office confidence in the identity of the bearer and to help maintain the security of Canadian passports.

The complaint was considered not well-founded.

On-line security of taxpayers' information

A Chartered Accountant challenged the security of the Canada Revenue Agency (CRA)'s on-line system. She complained that the existing system could improperly disclose taxpayers' information. Individual taxpayers do not have to ask for on-line access—it is available by default. She argued that CRA has put the onus on taxpayers to protect their information. Instead it should require taxpayers wanting on-line service to register, and should then enhance the security requirements.

In October 2003 CRA introduced a program allowing taxpayers to access their 2001 and 2002 tax information via the "My Account" section of CRA's Web site at www.cra-arc.gc.ca. To gain access, taxpayers have to supply their Social Insurance Number, date of birth, amount of income reported on line 150, and their eight-digit access code from their Notice of Assessment. Taxpayers can block on-line access to their information by getting in touch with CRA's e-help desk at the toll free number provided.

CRA also protects the information with encryption technology and security procedures. Taxpayers wanting to use the service must first install a secure browser which requires the taxpayer to use a personally assigned password.

The accountant also pointed out that with the exception of the date of birth, all the information required for on-line access is printed on the Notice of Assessment. Since taxpayers are frequently asked to provide the notices as proof of income by lenders,

credit card providers, financial advisors and other institutions, anyone with a copy could access the taxpayer's file. The complainant had no evidence of any unauthorized access.

The OPC concluded that CRA's security measures are sufficient to protect taxpayers' information in the system and the complaint was not well-founded. Also the *Income Tax Act* requires CRA to provide taxpayers with a Notice of Assessment. Once taxpayers receive the notice, the onus is on them to protect the information.

Creating Travel Profiles for Public Servants

A government employee complained about the amount of personal information that Public Works and Government Services Canada (PWGSC) collects in the Traveller Profile form.

The federal government has completely reorganized its method of arranging employees' travel. It created a Government Travel Modernization Office which subsequently awarded a contract to Accenture to deliver all government travel services. Accenture then subcontracted credit cards and travel services to American Express.

Government employees must now make all travel arrangements through Travel AcXess Voyage. But they must first complete a Traveller Profile in order to obtain the required Travel Identification Number before making any travel arrangements. The profile is sent to the credit card company, which then issues the number.

The information required included employees' group and subgroup, level, travellers' home telephone numbers and home addresses, emergency contact names, and dates of birth. The investigator reviewed the form and met PWGSC staff to determine why employees had to provide each of the details. The investigator also reviewed a PWGSC document explaining why the information was required. Eventually, the department agreed to the investigator's request to remove the date of birth and make optional the requests for emergency contacts and home telephone numbers.

The complainant reviewed the revised Traveller Profile form and was pleased with the deletion of the date of birth, and the now-optional requests for other details. He was also happy with the department's explanation of how the information is safeguarded and agreed that the case could be considered settled during the investigation.

Buying gallery ticket not an invitation to ongoing marketing

An art lover who purchased a ticket to the National Gallery's Klimt exhibit was disconcerted when called on to support the Gallery's ongoing programs. Shortly after buying the Klimt ticket, the complainant received a call from the National Gallery Foundation asking whether she had enjoyed the exhibit. She ended the call.

Some time later, when a foundation volunteer called again to solicit her support, the woman asked how they knew about her visit and why she was on the call list. Since the volunteer did not know, she asked the gallery directly. They revealed that they routinely disclose ticket buyers' information to the foundation for fund raising.

The woman complained to the Privacy Commissioner that the disclosure was improper. The investigator confirmed that the gallery builds a database from ticket sales for membership drives and to promote upcoming exhibits. The gallery removed her name from the database and apologized for the calls. It will also seek express consent in future before adding ticket purchasers' names to the foundation's database.

The woman was satisfied with the resolution of her complaint, which the Office considers settled in the course of investigation.

E-mail system confounds sender, discloses safety worries

A Statistics Canada employee complained that his supervisor's e-mail branding him violent and a threat to others' safety was an improper use and disclosure of his personal information. The e-mails between the supervisor and a human resources officer were available to all staff on the agency's internal network for five weeks.

The complainant had filed a harassment complaint against his supervisor. The e-mails discussed the supervisor's concern that the employee could become violent if given copies of her and other employees' witness statements about the harassment complaint.

Statistics Canada investigated the complaint as a possible breach of both its internal security and privacy policies. The agency's e-mail system allows users to designate their e-mails as normal, personal, private or confidential; however, the Document

Management Centre (DMC), which administers and maintains the electronic communication systems, does not routinely capture the designation.

The disputed e-mail was sent through the DMC using the Agency Messaging Options which offers a “Complete Send” or, if senders select the “Options” function, two other possibilities. Senders can select an “Accessibility Option” which allows them to determine the message’s level of security and distribution, or the “Access Restriction Option” which allows a “read only access”. Senders can also tell the DMC what level of access they want. However, they will only be aware of these choices if they select the Options function at the outset.

The supervisor had attempted to classify her message by flagging it “Private” or “Confidential” through Microsoft Outlook. She had not understood that she also needed to flag it as “Protected” for the DMC. The DMC procedures require its classifiers to check the header information, analyze the contents, check the security level and verify with the sender if the security is unclear. The message is then sent to appropriate recipients.

Two factors contributed to the inappropriate disclosure; the supervisor’s misunderstanding of the system’s method of controlling access—disclosure was not intentional, and the DMC’s failure to properly classify the message before putting it on the system.

Following the complaint investigation, Statistics Canada issued agency-wide instructions on assigning security levels to e-mails. The agency is also considering having DMC personnel staff review any Outlook e-mail that is flagged with security designations before putting them in the database. Longer term, StatsCan will review the DMC’s workings and protocols on personal information and report progress to the Office.

The Office concluded that the complaint was well-founded but, given the work underway on the e-mail system, the Office need take no further action.

Incidents under the *Privacy Act*

Over and above individual complaints, incident investigations are conducted into matters of improper collection, use or disclosure of personal information that come to the attention of our Office from various sources including the media and directly from departments themselves. They often highlight a systemic issue, or an

unrecognized privacy breach that needs to be fixed as soon as possible. Last year, the Office completed 27 investigations into mismanagement of personal information. Of these, five incidents concerned individuals receiving someone else's information. All were determined to be isolated incidents and prompted renewed vigilance among government employees.

Two cases of interest are described below.

Gardener Finds Income Tax Information

Several incidents involved stolen information. For example, early in 2004 a Vancouver Parks Board gardener found a bag containing income tax information under the False Creek Bridge. The bag contained 12 bundles of taxation remittance slips from two financial institutions. The slips contained the name, address, payment amounts and account numbers of various individuals and businesses. Only two of the bundles had been opened but all the documents were wet and had been exposed to the elements for some time. This information had been processed directly by a private clearing house on contract to the two financial institutions. The bag is believed to have been stolen in transit from the financial institutions to the Canada Revenue Agency.

At the time of the theft, the agency determined that the stolen bag contained 1,600 remittance vouchers. While the majority of the vouchers concerned businesses, 390 were from individuals. Since the clearing house did not plan to contact any of the affected individuals, the Agency on its own initiative notified the clients of the theft so that they could take steps against identity theft. Our Office confirmed that clients had indeed been notified at the time of the theft so that they could take appropriate steps against identity theft. All information was apparently recovered and no individual privacy complaints were received relating to this theft. The Privacy Commissioner commends the Agency for its initiative in protecting the privacy of its clients, even though it was not responsible for this particular privacy breach.

Photos of CSC Employees Appear in CBC Story

A Correctional Officer of the Correctional Service Canada (CSC) reported that on November 16, 2004 he had seen a photograph of himself and some of his colleagues on a CBC Web site in a story entitled "*Ombudsman Looking into Abuse at Prison Unit*".

The CSC's Web site has a "Photofile" containing various photographs of penitentiaries, CSC office buildings, and correctional officers at work. The photos are intended to provide the media with photographs to illustrate news articles. Also on the CSC site and therefore publicly available is a CSC employee publication entitled *Let's Talk* which often contains photographs of employees at work.

In this case, the CBC was preparing a story on allegations that correctional officers were abusing inmates in the segregation unit at Kingston Penitentiary. The CBC obtained a group photograph of several correctional officers from the CSC site, which it used to illustrate its story about abuse in the segregation unit. Although the individuals had nothing to do with the unit, by using the photo in this context, the CBC left the impression that they did.

The CSC contacted the CBC which removed the offending photographs from its site. The CSC also removed the disputed photos from its "Photofile". It then examined each remaining photograph to ensure that the individuals signed proper waivers before it displayed the photos on the site. However, CSC recognized that the waivers would have to be updated to ensure that employees knew that once their photographs were on the Web site, they could be reproduced and used for purposes other than simple articles about CSC. The department conducted extensive internal discussions with management and legal services on employee consent. CSC also temporarily withdrew *Let's Talk* from the site until all the issues were resolved.

The "Photofile" is now on the CSC site but it no longer contains any photographs of individuals. *Let's Talk* has also returned to the CSC site but the photographs only depict people who have signed express consent/waiver forms.

Public Interest Disclosures under the *Privacy Act*

Paragraph 8(2)(m) of the *Privacy Act* gives heads of government institutions the discretion to disclose personal information without the individual's consent when the disclosure benefits the individual or when a compelling public interest outweighs

the invasion of the individual's privacy. The head of the institution is required (under subsection 8(5)), to notify the Privacy Commissioner of such disclosures, preferably in advance (unless some urgency dictates otherwise). The Office reviews the disclosures and, if deemed necessary, the Privacy Commissioner notifies the individual to whom the information relates. During the review process, the Office also advises institutions when it believes more personal information than is necessary to address the public interest is proposed for release. In this way, we minimize the intrusion into the individual's life.

Last year we reviewed 76 such notices, a large number of them in two categories. The first concerns disclosing the circumstances of death to family members. We received 24 notices of this type, the majority of which came from the CSC and National Defence.

The second significant volume – 21 – came from the RCMP and the CSC concerning individuals who were either unlawfully at large or being released from custody at the end of their sentences. All are considered at high risk to re-offend and therefore a danger to the community.

Another 11 notices dealt with disclosures to Parliamentary Committees, Boards of Inquiry or other public entities on matters such as the sponsorship program, possible misconduct by public servants, or the circumstances surrounding accidental deaths.

Also of interest were four notices from Health Canada concerning health risks to the public from individuals with communicable diseases, two notices to the Children's Aid Society concerning possible child abuse, and four notices of security threats.

Inquiries

The Inquiries Unit responds to requests for information from the public about the application of the *Privacy Act* as well as *PIPEDA*. In this reporting year the unit responded to almost 3,000 inquiries solely dealing with matters pertaining to the *Privacy Act* and responded to some 17,000 requests for information under *PIPEDA*. In the course of the year, staff shortages in the Inquiries Unit coupled with the ongoing heavy volume of work have presented challenges. As a result it was necessary to reassess the way we respond to public inquiries. We no longer accept or respond to inquiries or complaints by e-mail. We introduced an automated telephone system to answer the public's most frequently asked questions such as those about identity theft, telemarketing and, of course, the social insurance number. And we continue adding

information to our Web site to answer the most frequently asked questions. We also temporarily assigned some investigators to help the unit. Lastly, we now invite individuals to telephone during office hours since we can often determine a caller's needs faster and better in person than in a series of e-mails and letters.

INQUIRIES STATISTICS

(April 1, 2004 to March 31, 2005)

The following table represents the total number of *Privacy Act* inquiries responded by the Inquiries Unit.

Telephone inquiries	2,391
Written inquiries (letter, e-mail, fax)	585
Total inquiries received	2,976

Inquiries Response Times

Eighty per cent of inquiries were received by telephone. The majority of these were responded to immediately; the remainder which may have required research were responded to within one to two weeks.

Written inquiries accounted for 20 per cent of the workload and, on average, were responded to within three months. Providing written responses to inquiries may be time consuming and labour intensive. Over the year, the Inquiries Unit accrued a backlog of written inquiries which exacerbated the average monthly turn around times. In the next fiscal year, we plan to implement new measures and to obtain additional resources to respond more quickly to the public's queries.

Audit and Review

Strengthening the Audit Function

The *Privacy Act* empowers the Privacy Commissioner (in subsection 37[1]) to investigate some 150 government institutions' compliance with sections 4 to 8 of the Act. These sections set out federal government obligations when collecting, retaining, disposing of, and protecting personal information. The Act also authorizes the Commissioner to audit certain databanks that are exempt from individual access.

In March 2005 the Office re-named its compliance review branch Audit and Review. This signals an important change. The Office has not used its audit powers to their full potential in assessing the quality of privacy management, or addressing the risks inherent in current federal operations. In the past year we began rebuilding and re-enforcing the audit and review functions. We intend to make greater use of audits and they will become an important tool in carrying out our mandate pursuant to the *Privacy Act* and *PIPEDA*.

Our Office's goal is "to conduct independent and objective audit and review of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability".

It will take time to build sufficient audit capacity, as well as meet departments' demand for timely reviews of privacy impact assessments as Treasury Board policy requires. In preparation, we have taken the following steps:

- Completed an external review of audit methods and practices;

- Set a branch goal and articulated team values;
- Began developing a longer term audit strategy and plan in view of privacy risks and issues;
- Built a business case to increase audit and review resources;
- Raised awareness with Parliamentary Committees on the potential of privacy auditing; and
- Improved audit practices as part of the audit of the CBSA (see below).

Auditing Cross-Border Flow of Personal Information

As mentioned earlier in this report, improving border security became a top priority for Canada and the United States following the events of September 11, 2001. A number of national security measures were instituted under the December 2001 Manley/Ridge Smart Border Declaration and 30-Point Action Plan.

Since then the government has allocated approximately \$10B for national security programs and initiatives. Over \$1.7B of that amount was given to the CBSA to implement measures aimed at strengthening land, marine, airport, and border crossing infrastructures; increasing the agency's human resource base; and improving its detection tools.

Canada and the U.S. also committed to enhancing border enforcement by exploring options for exchanging information and making better use of technology. The CBSA and the United States Department of Homeland Security (DHS) have worked on several initiatives that deploy technology and resources to better manage risk at the Canada-U.S. border. The initiatives include joint enforcement, joint-screening facilities, coordinated intelligence, and integrated databases to allow sharing of intelligence.

However, the Canadian public is concerned about the flow of personal information to the U.S. Media reports have indicated that Canadians are not willing to trade their privacy for measures which do not clearly enhance their security. This has been supported by an EKOS Research Associated survey commissioned by our Office, which indicates that 75 per cent of Canadians surveyed believe Canadian government agencies transfer citizens' personal information to foreign governments in order to protect national security, and with that 85 per cent of those surveyed reporting a moderate or high level of concern about such transfers.

Privacy and human rights advocates and Canadian politicians have all raised concerns about the implications of transferring personal data across international borders.

Among the concerns are data mining, racial profiling, direct access to databases by American authorities, secondary uses of information, matching data with private sector information, and the potential of the *USA PATRIOT Act* overriding Canadians' privacy rights.

Given this context, in July 2004 our Office notified the President of the CBSA that it intended to audit the Agency's management of the trans-border flows of personal information under its control.

The objective of the audit is "to assess the extent to which the CBSA is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or institutions thereof". The audit will focus on exchanges of information between Canada and the U.S. A key element will be to map (to the extent practicable) the information about Canadians that the CBSA transmits to the U.S. and for what purpose.

We believe that national security objectives and sound personal information management practices are mutually dependent. Rigorous controls over the gathering and use of personal information will limit such privacy risks as improper uses or disclosures, and also support a robust national security objective. Relevant, timely and accurate information sharing is the life-blood of enforcement and intelligence operations. However, sharing must take place with the highest standards of privacy and security protection to prevent losing credibility with the public, Parliamentarians and foreign partners.

The general criteria guiding the audit are that collection, use and disclosure of personal information must be limited to that which is necessary and permissible by law. They should also be circumscribed by multiple layers of privacy and security protections during the life-cycle of the information so as to prevent and mitigate risks to personal privacy and program objectives.

The CBSA's customs and immigration enforcement programs require it to collect, use and disclose considerable sensitive personal information. The information might include financial, family history, health, and travel information; personal identifiers such as the social insurance number, immigration and passport numbers; and biometrics digital photographs, fingerprints and iris scans.

Due to the CBSA's size and complexity, our Office has spent most of its limited audit resources on determining which of the agency's many programs and information

management activities have the greatest impact on individuals' privacy. The Office will focus its audit on these areas.

To better understand the CBSA's business, the audit team has reviewed open source information, descriptions of CBSA programs and activities, internal policies on managing personal information, applicable training materials, information flow-charts, information sharing agreements, privacy impact assessments and IT system descriptions. The team interviewed selected personnel at headquarters and several regional operational units. We observed customs officers at the primary inspection line and secondary examination areas. The team was also briefed on the electronic systems used at land borders and airport terminals to assess whether a traveller or passenger poses a risk.

This phase of the audit was completed early in the 2005 fiscal year. Examination is began in May 2005 and an audit report completed by January 2006.

Other Audit and Review Activity

HRSDC databank reviews

Since 2001, our Office has reviewed about 60 data linkage proposals by Human Resources Development Canada (now Human Resources and Skills Development Canada–HRSDC and Social Development Canada–SDC). These reviews are mandatory under a *Governance Protocol* that came into force in 2000 following significant concerns about HRDC's Longitudinal Labour Force File (since dismantled). The protocol governs all future research involving data linkage.

The quality of data linking proposals submitted to our Office has increased significantly—to the point that we rarely find it necessary to give advice to HRSDC. The department has developed the internal capacity to identify and respond to privacy risks associated with data linkages for research and program evaluation. The *Governance Protocol* is a model we encourage other departments and agencies to adopt.

Accordingly, in March 2005 our Office wrote to both departments recommending that their review of data linkage proposals be made optional and at the departments' discretion. The departments adopted the recommendation and will make the necessary amendment to the *Governance Protocol*. We proposed the change on the understanding that the departments would maintain the integrity of structures and procedures. We also expect SDC and HRSDC to minimize any potential disruption on the internal review caused by the separation of their responsibilities. Finally, we

encourage personnel from both departments to share their knowledge and experience with colleagues from other departments and agencies. This should reinforce their capacity to assess the privacy impact of any form of data matching or linkage.

Given HRSDC and SDC's large and complex systems which contain extensive personal information, we expect to conduct a future audit to determine whether their privacy management frameworks are sustained and continue working effectively.

Data Matching

Under the Treasury Board Secretariat (TBS) of Canada's *Policy on Data Matching*, federal departments and agencies are required to notify the Office of any data matching proposal. The purpose is to afford the Office an opportunity to review and comment on such proposals.

Given the small number reported to us, our concern is not so much the data matching proposals that take place, but the risk of data matching that is unreported and/or not subject to assessment. Information obtained from TBS indicates that there is confusion among departments as to the meaning of data matching that may contribute to under reporting of such activity. TBS is now addressing the confusion. We share the concern and favour a clear and comprehensive definition that would capture the activity in various forms whether called data matching, linking or mining.

At the moment, it is not clear if the federal government has a handle on the extent of actual "data matching" of personal information, including activity carried out by third parties engaged under contract with the federal government, and whether they are in keeping with legislation, policy and good personal information management practices. We will continue monitoring developments and consider the possibility of carrying out a future audit in this subject matter area.

Follow-up review of the Canadian Firearms Program

The Office first reviewed the Canadian Firearms Program in 2001. Since then, we have monitored developments (see pp. 49-50 of Annual Report 2003-04). As the result of ongoing negotiations to improve practices, last year we received a positive response from the now Department of Public Safety and Emergency Preparedness Canada indicating that they had taken steps to address our concerns. These include better written agreements with contractors to protect personal information, limiting access to municipal and provincial police information retrieval systems to a need to know basis, reiterating that it will not disclose personal information to employers, and improving consent forms.

However, given the passage of four years, the controversy surrounding the program, and the many ensuing changes, including recent amendments to the *Firearms Act*, it is time to refresh our knowledge of the program in order to plan a new audit.

Privacy Impact Assessments

The Treasury Board of Canada requires federal departments and agencies to conduct Privacy Impact Assessments (PIAs) on all new government programs or services that raise privacy issues. Assessments are also required when departments substantially change existing programs and services so as to require new or increased collection, use or disclosure of personal information. Departments must also assess new data matching, contracting-out or other changes that may have privacy implications.

The Treasury Board PIA policy is critical to protecting privacy. And, despite their inconsistent quality and thoroughness, PIAs have improved considerably. The improvement trend continued last year. We are particularly pleased that departments are increasingly including action plans in their PIA submissions. This is an encouraging sign that the PIA policy is having its intended impact; ensuring that government adopts privacy as a core consideration in planning, designing, and implementing programs and services.

Implementing a strategy to meet the PIA policy's requirements is a key component of any departmental privacy management framework. The policy itself promotes adopting a privacy governance structure. For example, the policy guidelines establish the accountabilities that form the core of a privacy management framework. The guidelines expect departmental heads to define the roles of personnel on adhering to the policy's requirements. The departmental heads must also assume responsibility for overseeing implementing the requirements.

We continue encouraging departments to establish a formal administrative structure that will review departmental initiatives to determine whether they require a PIA. The structure or bodies should define responsibility for issuing departmental directives and guidelines on compliance with the policy's objectives, and establishing bodies to manage PIAs. The bodies would review proposals to determine whether assessments are required; oversee and coordinate their conduct, consult with relevant stakeholders, approve recommendations, and monitor implementation of the recommendations.

Departments should also consult Treasury Board Audit Guides, particularly the section in the PIA Audit Guide entitled "Management Control Framework", which outlines appropriate administrative structures to support the policy.

As part of our review of PIAs (as required by Treasury Board Policy) we routinely ask departments to report the actions they will take in response to our recommendations and we will assess compliance with the policy's requirements and objectives in any future audit.

Treasury Board scheduled a comprehensive review of the PIA policy in May 2007, five years after its official launch. However, the Board seized the initiative – conducting an interim review of a small sample of federal departments and programs in June 2004. This early start allows the Board to assess the impact on privacy compliance, and identify any potential improvements. The Board consulted relevant stakeholders (including our Office) during the review. We concur with most of the study's findings and recommendations.

The study concluded that the policy had indeed enhanced privacy compliance significantly in the selected departments. There are, understandably, several areas requiring attention. These include, for example:

- acquiring the expertise needed to conduct PIAs;
- coordinating and integrating the contributions of stakeholders;
- documenting observations with the necessary evidence;
- harmonizing PIAs with other government policies, such as the government's security, data matching, and social insurance number policies; and
- making PIA summaries publicly available.

The study also concluded that our Office's oversight and advisory role is critical to ensuring both the integrity of the assessment process and public confidence in the policy. However, our ability is compromised by a lack of resources. We welcome the study's acknowledgment of the need to provide adequate funding. The matter will form part of an overall business case for permanently funding our Office planned for submission to the Treasury Board later in 2005.

Treasury Board's study also found no single reliable source of information on how many assessments have been conducted. Nor is there a sufficiently complete mechanism in place for ensuring assessments is always conducted on initiatives that would warrant such analysis. Departments need to improve their monitoring and reporting, and their annual reports appear to be the appropriate method.

In April 2005 Treasury Board issued revised reporting guidelines for fiscal year 2004-2005 regarding annual reports on the *Access to Information Act* and the *Privacy Act*. We are pleased to see the guidelines now require departments to report on the number of PIAs and preliminary assessments conducted during a fiscal year.

Given indicated shortcomings, we are considering auditing the functioning of the whole PIA system. We are concerned that assessments are not being done when they should. And we need to determine whether systems and procedures are working to ensure departments follow through on the assessment findings as part of their privacy management program or framework.

In the Courts

Privacy Act Applications

Once the Privacy Commissioner has investigated a complaint, Section 41 of the *Privacy Act* allows the individual to apply to the Federal Court for review of the government's refusal to provide access to personal information. The following applications were filed in the past fiscal year:

1. Keith Maydak v. Solicitor General of Canada (Federal Court file No. T-972-04)
2. James R. Gairdner v. Jennifer Stoddart et al (Federal Court file No. T-2005-04) Discontinued February 2005

Section 42 of the *Privacy Act* also allows the Commissioner to appear in Federal Court. The Commissioner may ask the Court to review an institution's refusal of access to personal information (with the complainant's consent). She may act on behalf of individuals who have applied for review themselves, or with the leave of the Court, be a party to any review sought under section 41. The Privacy Commissioner did not appear in court in any of these capacities in the past fiscal year.

The Privacy Commissioner can also become involved in applications where the complainant improperly names the Commissioner as a respondent and tries to seek relief against her that is not available. The following two such cases were decided in the fiscal year:

Gauthier v. Canada (Department of Justice) and Privacy Commissioner of Canada

Federal Court File No. T-653-02

Mr. Gauthier requested that the Department of Justice provide him with access to all personal information about himself. After consultations with a variety of other institutions, the Department provided him with a total of 685 pages of information and advised that some information had been withheld under sections 26 and 27 of the *Privacy Act*. Mr. Gauthier complained to the Privacy Commissioner that the Department was improperly withholding his personal information.

The former Privacy Commissioner reviewed the information which had been withheld and agreed that the section 26 and 27 exceptions had been properly applied and thus that the complaint was not well-founded. Nevertheless, the Commissioner asked Department of Justice to reconsider its exercise of discretion with respect to some of the information, upon which information was released to Mr. Gauthier.

Mr. Gauthier filed an application under s. 41 of the *Privacy Act* in which he asked improperly for, among other things, review of the findings of the Privacy Commissioner with regard to his complaint.

In October 2003, the Interim Privacy Commissioner filed representations regarding the lack of Court jurisdiction to review the findings of the Privacy Commissioner.

A hearing was held on March 31, 2004, at which time Mr. Gauthier conceded that he was not in fact seeking a review of the Privacy Commissioner's findings but only of the decision of the government institution to refuse to provide him with access to all his personal information. In a decision which reviewed the principles of solicitor-client privilege and determined that some of the information should have been released, the Application against the government was allowed in part on May 4, 2004.

Mamidie Keïta and Bernard Michaud v. The Minister of Citizenship and Immigration Canada and the Privacy Commissioner of Canada

Federal Court File No. T-676-03

The complainants had sought personal information in all Citizenship and Immigration Canada offices, especially embassies in Guinea, the Ivory Coast, Ghana and Senegal. Dissatisfied with the response from CIC, they lodged a complaint with the Privacy Commissioner, who investigated and concluded that the complaint was well-founded

at the time it was lodged. However, since CIC provided the complainants with the additional information to which they were entitled in the course of the investigation, the Privacy Commissioner considered the complaint resolved. The Commissioner agreed with CIC that the remaining information withheld from the complainants was third party information which was exempt under section 26 of the *Privacy Act*.

The complainants then filed for a Court review under section 41 of the *Privacy Act*. Since the application improperly named the Privacy Commissioner of Canada as a respondent, the Interim Privacy Commissioner filed a motion in July 2003 requesting that he be struck from the application. The Court dismissed the motion suggesting that the issue was overly complex in this case and best dealt with at trial.

The Application was dismissed on April 28, 2004, with the Court reiterating that the Applicants cannot, by means of a review application against the government institution, also obtain judicial review of the Commissioner's recommendations. The Court also confirmed that the section 26 exemptions were proper and that the Applicants had received all the personal information to which they were entitled.

Judicial Review

Complainants will sometimes seek judicial review under section 18.1 of the *Federal Courts Act* against the Privacy Commissioner. This occurred in the case described below, where the Commissioner was required to explain her jurisdiction to the Court when the complainant sought remedies that the Commissioner had no authority to grant. This case illustrates the seriously limited remedies available under the *Privacy Act* for any breaches other than improper denials of access. The Commissioner finds herself in the unenviable position of having to demonstrate to the court how she is unable to help the complainant. Clearly, this is an important issue for *Privacy Act* Reform.

Brian Murdoch v. Royal Canadian Mounted Police and Privacy Commissioner of Canada

Federal Court File No. T-1180-04 and Federal Court of Appeal File No. A-183-05

Mr. Murdoch complained to the Privacy Commissioner, that among other wrongful conduct, the RCMP had breached the *Privacy Act* by disclosing his personal information to his employer without his consent. The Assistant Commissioner responsible for the *Privacy Act* agreed that his disclosure complaint was well-founded.

On June 18, 2004, Mr. Murdoch sought a judicial review of the Assistant Commissioner's report on his disclosure complaint. Although the *Privacy Act* restricts remedies to questions of access, he argued that the Privacy Commissioner must necessarily have the authority to fashion remedial orders and relief in cases (like his) where the Act has been contravened.

On June 29, 2004, the Privacy Commissioner filed an objection to Mr. Murdoch's request that she provide him a certified copy of all material and relevant documents in her possession. In August 2004 she moved to strike the application. However, the Court denied the motion in September 2004 noting that the merits of the Privacy Commissioner's argument (that she has no authority or jurisdiction to grant the remedies sought) could easily be determined when the Court heard the application.

At a hearing in March 2005 the Court determined that the Privacy Commissioner had fulfilled her obligations under the *Privacy Act* and had correctly advised the applicant that the Act provides no penalty to address the respondent's breach of his privacy. The applicant can obtain no further award in the Court for the improper disclosure.

Mr. Murdoch appealed the Federal Court decision in April 2005.

Public Education and Communications

The Office of the Privacy Commissioner of Canada is mandated specifically under *PIPEDA* to develop and conduct information programs to foster public and organizational understanding and recognition of the rules that govern the collection, use and disclosure of personal information. And although there is no legislative mandate for public education specified under the *Privacy Act*, there is certainly a mandate to ensure departments and agencies are held accountable for their personal information handling practices. There is often a necessity to inform the public, as well as departments and agencies, about the requirements of the Act and related policies, and the impact on the privacy rights of Canadians of current and proposed government activities.

In 2004-2005, the Office undertook a strategic communications planning effort with the expertise of external consultants, and the result was a comprehensive communications and outreach strategy for the coming fiscal years. This strategy will enable the Office to have a more comprehensive, proactive approach to communications planning and delivery; a more truly public education-focused approach to communications surrounding *PIPEDA*; and build a greater level of awareness of the Office and of key privacy issues under both laws.

In addition to developing this strategy the Office undertook the following communications activities in 2004-2005:

Speeches and Special Events

Speaking engagement opportunities have helped our Office raise awareness of privacy issues among diverse audiences and settings, including professional and industry associations, non-profit and advocacy groups and universities. In 2004-2005, the Commissioner, Assistant Commissioners and other senior officials delivered

21 speeches, speaking out about issues with privacy implications, such as security initiatives and health care delivery.

In March 2004, the Office began hosting an in-house Lecture Series (approximately one per month). These information sessions featured experts on a variety of privacy issues and brought together members of the privacy community and staff. In 2004-2005, the Office hosted nine of these information sessions.

Media Relations

Privacy issues continued to be of interest to the media in 2004-2005, with significant coverage in Canada on issues such as privacy and security, about which the Office received media calls and participated in interviews. In addition, through other proactive media relations efforts, such as the dissemination of news releases, the Office had the opportunity to raise awareness of, for example, the launch of its Contributions Program; the Commissioner's views on important legislation, such as the do-not-call list legislation; and the Office's views regarding transborder flows of personal information.

Web Site

We post new and useful information on our Web site on an ongoing basis. Fact sheets, news releases, speeches, case summaries of findings under *PIPEDA*, are posted to keep the site interesting to individuals and institutions. In 2004-2005, the Office redesigned its Web site in order to make it compliant with the Common Look and Feel standards established by Treasury Board. This resulted in an enhancement to the design as well as to the navigation tools on the site, in order to help visitors make better use of the site. The Office also made the site more dynamic with the posting of a downloadable Web-video for businesses on complying with *PIPEDA*. Since 2001-2002, we are pleased to report that visits to the site have more than quadrupled, reaching 904,886 in 2004-2005.

Publications

The Office has produced information materials, including guides for individuals and institutions on *PIPEDA*, as well as a variety of new fact sheets on issues including consent, use of the social insurance number in the private sector, transborder flow of personal information, and how our Office conducts investigations into potential privacy breaches.

In 2004-2005, in addition to preparing new fact sheets, we developed an e-kit for businesses to help them comply with the new law. We also revised the content of

our guides, to ensure they were up-to-date given the final stage of implementation of *PIPEDA* on January 1, 2004. We received requests for these materials on a daily basis. Not only were these materials sent to individuals upon request, they were also distributed at conferences and special events, and accessed in electronic format by visitors to our Web site. In 2004-2005, close to 22,000 of our publications (guides, fact sheets, annual reports, copies of both federal privacy laws) were sent out, in addition to the more than 635,000 publications which were downloaded from our Web site.

Internal Communications

Internal communications activities were also a focus of the Office and played a key role in 2004-2005, increasing transparency between management and staff, especially during its ongoing institutional renewal, but also through day-to-day activities. Internal communications activities in 2004-2005 involved providing staff with information on, for example, human resources issues, upcoming speaking engagements, Parliamentary appearances, senior management and labour management committee meetings, and special events such as all-staff meetings and information sessions. The Office has been developing an Intranet, an internal communications portal to host all internal communications and maximize staff access to information, which will be launched in 2005-2006.

In the upcoming year, the Office will continue to undertake the activities outlined above. We also hope to be in a position to initiate many of the more proactive public education activities outlined in the communications and outreach strategy.

Corporate Services

On the Path to Institutional Renewal

The Commissioner's most immediate priority has been to lead the Office's institutional renewal by strengthening OPC management processes, particularly human resources and financial management – planning, budgeting, reporting and control mechanisms.

Planning and Reporting

A foundation component of the Office's institutional renewal is a strategic planning, reporting and control process. During 2004-05 we completed our first year under this revised process. The strategic plan established at the beginning of the year was our road map for the year. As part of the new process were reporting and review opportunities. We made adjustments to plans and budgets throughout the year. To assist in our reporting and reviews we developed a Performance Measurement Framework and a monthly performance report. We also launched a Business Process Review of the entire institution which will enable the Office to better estimate resource requirements and to draft a business case for permanent funding.

Human Resources

We continue to work toward the development and implementation of changes to improve how the office is run and the quality of the workplace. Significant changes and improvements have been made to the Human Resource management policies and practices.

We developed a number of Human Resource policies in consultation with central agencies and unions. These policies will guide us as we build on the successes of the past year and we continue on our path of institutional renewal. An Instrument

of Delegation of Human Resource Management was developed and will serve as a tool to inform and guide managers, and enable them to manage their human resources. A new Strategic Human Resource Plan and Staffing Strategy, as well as an Employment Equity Action Plan, will help the OPC achieve its mandate and ensure the recruitment of a highly qualified workforce that is diversified and representative of Canadian society. As part of OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed on a monthly basis to all staff.

Over the course of the past fiscal year we made significant strides in the area of organizational learning, including the development of a learning strategy with the Canada School of Public Service (CSPS), training and information sessions in values based staffing, language training sessions, performance management and employee appraisals and harassment in the workplace. The development and implementation of a Learning Strategy and Curriculum with the CSPS will enable staff to continue to develop the expertise and competencies required to fulfil their functions, as well as to position staff to take on new responsibilities and accountabilities.

We continued to work collaboratively with Central Agencies such as the Public Service Commission and the Public Service Human Resources Management Agency of Canada on follow-up measures to the recommendations of the Public Service Commission and the 2003 report of the Auditor General of Canada. This included measures that will allow OPC the opportunity to regain its full staffing delegation authority.

Finance and Administration

The OPC received a clean opinion on Audited 2003-2004 Financial Statements by the Office of the Auditor General of Canada. This is a significant milestone and a very positive indicator that the institution has indeed advanced on the path of institutional renewal. The institution has built on that success by establishing planning and review cycles, by streamlining and improving the financial management policies and practices.

Information Management / Information Technology

Significant advancements have also been made in how we manage our information assets. We completed an audit of our information management systems and we completed a vulnerability assessment of our information technology. We also completed an information technology strategy. This will help us to not only meet our obligations with respect to the management of government information and security policies, but

more importantly it will guide us as we move forward in improving on the management of our information assets. During the year we completed a significant upgrade to our case tracking and reporting system, Integrated Investigations Application (IIA). Finally we also established the framework for an internal Intranet site. This site will allow for effective communicating and sharing on information for employees.

Down the road

Strategic planning is an important annual exercise for the OPC. Our last session in January 2005 provided managers and employees an opportunity to re-examine the OPC's priorities for 2005-2006, and the actions they would take to achieve these priorities.

Corporate Services priorities for 2005-2006 are to:

- Develop and implement a Management Accountability Framework (MAF);
- Implement and maintain a human resource strategy that enables the Office to recruit, retain and develop staff and foster a continuous learning environment;
- Satisfy central agencies' requirements to regain delegated authorities, and enable the Office to take on new delegation to implement the Public Service Modernization Act;
- Develop and implement integrated information management;
- Complete Business Case for Resources for the OPC;
- Review Corporate Services Branch and Human Resources Branch policies and procedures; and
- Continue providing effective integrated financial services to the OPC.

Our Resource Needs

At the beginning of fiscal year 2004-2005, the Office's budget was \$11.2 million, the same as the previous year. Included was \$6.7 million for the Office's *PIPEDA* activities. Ongoing funding of OPC activities continues to be extremely important.

With privacy rights continually under threat, the Office's operations need to be funded adequately so that it is prepared to address the multitude of emerging privacy issues in the public and private sector.

The Office does not have adequate resources to fully exercise its powers and responsibilities under both Acts. Without adequate permanent funding, the Office cannot:

- Reinforce our audit and review functions to effectively address compliance under both privacy laws or strengthen our capacity to monitor, research and respond to emerging issues of technology and privacy;
- Conduct outreach and public education to influence change so policies and programs are viewed through a privacy lens;
- Continue investigating in a timely manner and resolving the growing number of complaints under both Acts; and
- Continue providing specialized legal and strategic advice and litigation support under both federal privacy laws, as well as strengthening established approaches and procedures to deal with cross-jurisdictional complaints.

To this end, the Office's priority beginning in the last quarter of fiscal year 2004-05 was to completely review all business processes. The review included establishing workload indicators and reviewing the legislative requirements, as well as external and internal factors that have an impact on our operations. This will enable the Office to develop a Business Case and make a formal submission to the Treasury Board Secretariat and to Parliament later in 2005 to stabilize our resource base and seek permanent funding for the Office.

We hope that with adequate permanent funding, the Office can further assure Parliament that it is effectively ensuring respect for Canadians' privacy rights in the public and private sectors.

Financial Information

April 1, 2004 to March 31, 2005

	Expenditure Totals (\$)	% of Totals
<i>Privacy Act</i>	3,745,058	32
<i>PIPEDA</i>	6,849,650	58.5
Corporate Services	1,107,296	9.5
Total	11,702,004	100

Note: Although OPC salary budget allows for approximately 100 FTEs (full-time equivalents), there were only 86 FTEs staffed at the Office at the end of March 2005.

Detailed Expenditures ⁽¹⁾	<i>Privacy Act</i>	<i>PIPEDA</i>	Corporate Services	Total
Salaries	3,330,147	3,039,732	419,120	6,788,999
Employee Benefits Program	190,327	844,575	154,640	1,189,542
Transportation & Communication	41,238	266,129	81,282	388,649
Information	1,907	147,911	5,239	155,057
Professional Services	171,783	1,397,579	210,403	1,779,765
Rentals	2,730	107,874	23,759	134,363
Repairs & Maintenance	4,698	155,805	85,353	245,856
Materials & Supplies	9,304	50,764	21,633	81,701
Acquisition of Machinery & Equipment	384	451,788	98,026	550,198
Other Subsidies & Payments	- 7,460	20,084	7,841	20,465
Transfer Payments	0	367,409	0	367,409
Total	3,745,058	6,849,650	1,107,296	11,702,004

⁽¹⁾ Total expenditure figures are consistent with the Public Accounts of Canada.

Financial Statements

The Management Responsibility letter and the audited financial statements as at March 31, 2005 will be available on our Web site at www.privcom.gc.ca in October 2005.

Nous espérons qu'avec un financement permanent, le Commissariat sera en mesure d'offrir une assurance renouvelée au Parlement pour veiller au respect du droit des Canadiennes et des Canadiens à la protection de leurs renseignements personnels dans les secteurs public et privé.

Renseignements financiers

Du 1^{er} avril 2004 au 31 mars 2005

	Dépenses globales (\$)	% du total
Loi sur la protection des renseignements personnels	3 745 058	32
LPPDE	6 849 650	58,5
Gestion intégrée	1 107 296	9,5
Total	11 702 004	100

Note : Bien que le budget salarial du CPVP ait permis environ 100 ETP (équivalent temps plein), le Commissariat ne comptait que 86 employés à la fin de mars 2005.

Dépenses détaillées ⁽¹⁾		Lot sur la protection des renseignements personnels		LPPDF	Gestion intégrée	Total
Salaires et traitements	3 330 147	3 039 732	419 120	6 788 999	1 189 542	
Cotisations au régime d'avantages sociaux des employés	190 327	844 575	154 640	1 189 542		
Transports et communications	41 238	266 129	81 282	388 649		
Information	1 907	147 911	5 239	155 057		
Services professionnels	171 783	1 397 579	210 403	1 779 765		
Locations	2 730	107 874	23 759	134 363		
Réparations et entretien	4 698	155 805	85 353	245 856		
Approvisionnement-ments et fournitures	9 304	50 764	21 633	81 701		
Achat d'appareils et d'équipements	384	451 788	98 026	550 198		
Autres subventions et paiements	- 7 460	20 084	7 841	20 465		
Paiements de transfert	0	367 409	0	367 409		
Total	3 745 058	6 849 650	1 107 296	11 702 004		

(1) Les dépenses globales correspondent aux données des Comptes publics du Canada.

États financiers

La lettre de responsabilité de la direction à l'égard des états financiers et les états financiers vérifiés en date du 31 mars 2005 pourront être consultés sur notre site Web www.privcom.gc.ca en octobre 2005.

www.privcom.gc.ca en octobre 2005.

Besoins en matière de ressources

Au début de l'exercice 2004-2005, le budget du Commissariat s'établissait à 11,2 millions de dollars, soit le même montant que celui de l'exercice précédent. De cette somme, 6,7 millions de dollars visent les activités du Commissariat à l'égard de la LPRPDE. Le financement des activités du CPVP est toujours un enjeu capital.

Compte tenu des menaces constantes à l'endroit du droit à la protection de la vie privée, les activités du Commissariat doivent être adéquatement financées de façon à ce que ce dernier prenne des mesures pour traiter la multitude des nouveaux enjeux en matière de protection de la vie privée dans les secteurs public et privé.

Le Commissariat ne possède pas les ressources adéquates pour exercer pleinement ses pouvoirs et assumer ses responsabilités en vertu des deux lois. Sans financement permanent suffisant, le Commissariat n'est pas en mesure de :

- renforcer ses fonctions de vérification et d'examen de façon à traiter efficacement l'application des deux lois régissant la protection des renseignements personnels, ou renforcer notre capacité de surveillance, de recherche et de réponse aux nouveaux enjeux en matière de technologie et de protection de la vie privée ;
- mener des activités d'information et de sensibilisation du grand public afin d'influer sur les changements pour que les politiques et programmes soient perçus selon un leitmotiv respectant la protection de la vie privée ;
- continuer à mener des enquêtes en temps opportun et à régler un nombre de plus en plus élevé de plaintes en vertu des deux lois ; et
- continuer à fournir des avis juridiques et stratégiques ainsi qu'un soutien juridique en vertu des deux lois régissant la protection des renseignements personnels, et renforcer les méthodes et procédures établies pour régler les plaintes entre les différentes juridictions.

À cette fin, la priorité du Commissariat au cours du dernier trimestre de l'exercice 2004-2005 a consisté à mener un examen de ses processus opérationnels à l'échelle de l'organisme. Il a donc fallu, notamment, établir des indicateurs de charge de travail et revoir les exigences législatives ainsi que les facteurs, tant internes qu'externes, qui ont une incidence sur les activités du Commissariat. Cela permettra au Commissariat d'élaborer une analyse de rentabilisation et de déposer un document de présentation officielle au Secrétaire du Conseil du Trésor et au Parlement, plus tard en 2005, en vue de stabiliser les ressources dont il dispose et de demander un financement permanent.

succès en mettant au point des cycles d'examen et de planification, de même qu'en simplifiant et en améliorant les politiques et les pratiques de gestion financière.

Gestion de l'information et technologie de l'information

Des progrès considérables ont également été accomplis en ce qui a trait à la gestion de nos ressources d'information. Nous avons terminé la vérification de nos systèmes de gestion de l'information ainsi qu'une évaluation de la vulnérabilité de notre technologie de l'information. Nous avons également élaboré une stratégie en matière de technologie de l'information. Cela nous aidera non seulement à remplir nos obligations dans le cadre de la gestion des renseignements administratifs et des politiques en matière de sécurité mais, surtout, à nous guider pendant que nous procédons à l'amélioration de la gestion de nos ressources d'information. Au cours de l'année, nous avons considérablement amélioré notre système de suivi des dossiers et d'établissement des rapports, l'Application d'enquête intégrée (AEI). Finalement, nous avons également mis au point un cadre pour un site intranet interne. Ce site permettra aux employés de communiquer et d'échanger des renseignements efficacement.

Pour l'année qui vient

La planification stratégique est un exercice annuel important au CPVP. Notre dernière session, en janvier 2005, a permis aux gestionnaires et aux employés de réexaminer les priorités du Commissariat pour 2005-2006, ainsi que les actions qu'ils entreprendront pour les mener à bien.

Gestion intégrée – priorités pour l'exercice 2005-2006 :

- élaborer et mettre en œuvre un cadre de responsabilisation de gestion (CRG) ;
- mettre en œuvre et maintenir une stratégie en ressources humaines qui habilitera le Commissariat à recruter, à conserver et à former le personnel, de même qu'à favoriser un environnement d'apprentissage continu ;
- satisfaire aux exigences des organismes centraux afin de recouvrer les pouvoirs délégués et de permettre au Commissariat d'assumer une nouvelle délégation afin d'appliquer la *Loi sur la modernisation de la fonction publique* ;
- élaborer et mettre en œuvre la gestion intégrée de l'information ;
- rédiger une analyse de rentabilisation des ressources pour le CPVP ;
- examiner les politiques et les processus de la Direction de la gestion intégrée et de la Direction des ressources humaines ; et
- continuer à procurer des services financiers intégrés efficaces au CPVP.

Nous avons élaboré un certain nombre de politiques de ressources humaines, en consultation avec des organismes centraux et des syndicats. Ces politiques nous guideront pendant que nous tirons profit de nos succès de la dernière année et que nous poursuivons notre cheminement vers le renouvellement institutionnel. Nous avons établi un instrument de délégation en matière de gestion des ressources humaines qui nous servira à informer et à aiguiller les gestionnaires et permettra à ceux-ci de gérer les ressources humaines. Un nouveau plan stratégique en matière de ressources humaines et une stratégie de dotation ainsi qu'un plan d'action sur l'équité en matière d'emploi aideront le CPVP à respecter son mandat et à assurer le recrutement d'effectifs hautement qualifiés, diversifiés et représentatifs de la société canadienne. En vertu de l'engagement du CPVP à faire preuve d'une meilleure transparence dans le processus de dotation, un bulletin du personnel a été mis sur pied ; il est distribué chaque mois à tout le personnel.

Tout au long du dernier exercice, nous avons fait des progrès considérables dans le domaine de l'apprentissage organisationnel, en élaborant notamment une stratégie d'apprentissage en collaboration avec l'École de la fonction publique du Canada (EFPC), des séances d'information et de formation sur la dotation en personnel fondées sur les valeurs, des séances de formation linguistique, des évaluations de rendement pour les gestionnaires et les employés et une politique sur le harcèlement en milieu de travail. L'élaboration et la mise en œuvre d'une stratégie d'apprentissage et d'un programme éducatif en collaboration avec l'EFPC permettront au personnel de continuer à développer son expertise et les compétences requises pour accomplir ses tâches, et l'amènera à assumer de nouvelles fonctions et responsabilités.

Nous avons continué à travailler en collaboration avec des organismes centraux tels que l'Agence de gestion des ressources humaines de la fonction publique du Canada et la Commission de la fonction publique du Canada sur des mesures de suivi, conformément aux recommandations de la Commission de la fonction publique et au rapport de la vérificatrice générale du Canada en 2003. Certaines de ces mesures donneront au Commissariat la possibilité de reprendre ses pleins pouvoirs de délégation en matière de dotation.

Finances et administration

Le Bureau du vérificateur général a émis une opinion favorable à la suite de la vérification des états financiers du Commissariat pour l'exercice 2003-2004. Voilà un jalon important et un indicateur que l'institution a effectivement progressé dans son cheminement vers le renouvellement institutionnel. Notre institution a profité de ce

Vers le renouvellement institutionnel

La priorité numéro un de la commission a été de diriger le renouvellement institutionnel du Commissariat en renforçant les processus de gestion du CPVP, en particulier la gestion des ressources humaines et la gestion financière – planification, budgétisation, établissement de rapports et mécanismes de contrôle.

La planification et l'établissement de rapports

Un élément de base du renouvellement institutionnel du Commissariat est la mise en place d'un processus stratégique de planification, d'établissement de rapports et de contrôle. En 2004-2005, nous avons conclu une première année sous ce processus révisé. Le plan stratégique élaboré en début d'exercice nous a servi de feuille de route tout au long de l'année. Les possibilités en matière d'examen et d'établissement de rapports faisaient partie de ce nouveau processus. Nous avons ajusté les plans et les budgets tout au long de l'année. Pour nous aider à établir des rapports et à procéder à des examens, nous avons mis sur pied un cadre de mesure du rendement et un rapport mensuel sur le rendement. Nous avons également initié une révision des processus pour l'ensemble de l'institution, ce qui permettra au Commissariat de déterminer avec plus de justesse les besoins en ressources et de rédiger une analyse de rentabilisation pour le financement permanent.

Les ressources humaines

Nous continuons à travailler à l'élaboration et à la mise en œuvre de changements en vue d'améliorer la façon dont le Commissariat est géré et la qualité du milieu de travail. Des changements considérables et des améliorations ont été apportés aux pratiques et aux politiques de gestion des ressources humaines.

Au cours de la prochaine année, le Commissariat continuera à prendre en charge les activités ci-haut mentionnées. Nous espérons également être en mesure d'entreprendre davantage d'activités de sensibilisation du grand public plus proactives dans notre stratégie en matière de communications et d'information.

la commissaire sur la conformité à la *LPRPD*. Il nous fait plaisir de signaler que depuis 2001-2002, le nombre de visites de notre site a plus que quadruplé, atteignant 904 886 en 2004-2005.

Publications

Le Commissariat a produit des documents d'information, dont des guides sur la *LPRPD* à l'intention des personnes, des organisations et des entreprises, ainsi que de nouvelles fiches d'information traitant de sujets tels que le consentement, l'utilisation du numéro d'assurance sociale dans le secteur privé, la circulation transfrontalière des renseignements personnels et la façon dont le Commissariat mène des enquêtes sur de possibles violations de la vie privée.

En 2004-2005, en plus de préparer de nouvelles fiches d'information, nous avons élaboré une trousse d'information électronique à l'intention des entreprises pour aider celles-ci à se conformer à la nouvelle loi. Nous avons révisé la teneur de nos guides afin de nous assurer que ceux-ci étaient à jour pour la mise en oeuvre intégrale de la *LPRPD* le 1^{er} janvier 2004. Nous avons reçu tous les jours des demandes au sujet de ces documents. Ceux-ci étaient acheminés aux personnes qui en faisaient la demande ou distribués lors de conférences et événements spéciaux, et les visiteurs de notre site Web pouvaient également les obtenir en format électronique. En 2004-2005, près de 22 000 publications du Commissariat (guides, fiches d'information, rapports annuels, copies des deux lois fédérales sur la de protection des renseignements personnels) ont été distribuées, sans compter les 635 000 publications téléchargées de notre site Web.

Communications internes

Le Commissariat a également mis l'accent sur les activités de communications internes, qui ont joué un rôle majeur en 2004-2005 en favorisant une plus grande transparence entre le personnel et la direction, en particulier pendant le renouvellement institutionnel en cours, mais aussi lors des activités quotidiennes. Les activités de communications internes en 2004-2005 consistaient à fournir au personnel des renseignements, notamment sur des questions en matière de ressources humaines, les discours à venir, les présentations devant le Parlement, les réunions des comités de la haute direction et de consultation patronale-syndicale et des activités spéciales telles que des réunions de l'ensemble du personnel et des séances d'information. Le Commissariat travaille actuellement à la mise sur pied d'un réseau de communications internes qui accueillera toutes les communications internes et maximisera l'accès à l'information pour le personnel. Le réseau sera lancé en 2005-2006.

Nous affichons de façon continue sur notre site Web des renseignements nouveaux et utiles. Des fiches d'information, communiqués, discours, résumés de conclusions d'enquêtes en vertu de la *LPRPDE* sont affichés sur le site afin de maintenir l'intérêt des personnes et des organisations. En 2004-2005, le Commissariat a restructuré son site Web afin qu'il soit conforme à la normalisation des sites Internet telle qu'elle a été établie par le Conseil du Trésor. Résultat : la conception et les outils de navigation du site ont été améliorés en vue de faciliter la consultation du site. Le Commissariat a également rendu le site plus interactif en y intégrant un discours téléchargeable de

Site Web

En 2004-2005, les médias ont continué à porter un intérêt soutenu sur la protection de la vie privée couvrant abondamment des questions telles la protection des renseignements personnels et la sécurité, comme le témoignent de nombreux appels médiatiques au CPVP et des entrevues accordées par ce dernier. De plus, grâce à d'autres efforts proactifs en matière de relations médiatiques, tels que la diffusion de communiqués de presse, le Commissariat a eu l'occasion d'entreprendre des activités de sensibilisation, notamment pour le lancement de son programme des contributions, pour faire connaître le point de vue de la commissaire sur d'importantes lois, tel le projet de loi visant à créer une liste nationale des abonnés auto-exclus, et pour communiquer le point de vue du Commissariat sur la circulation transfrontalière des renseignements personnels.

Relations avec les médias

En mars 2004, le Commissariat a commencé à présenter une série de conférences internes (en moyenne une par mois). Lors de ces séances d'information, des experts invités ont abordé diverses questions portant sur la protection des renseignements personnels devant des membres du milieu de la protection de la vie privée et devant le personnel du CPVP. En 2004-2005, le Commissariat a présenté neuf de ces séances d'information.

Les discours ont aidé le Commissariat à sensibiliser les divers auditoires et autres milieux aux enjeux relatifs à la protection de la vie privée, notamment des associations professionnelles et d'industries, des organismes sans but lucratif, des groupes de défense et des universités. En 2004-2005, la commissaire, les commissaires adjoints et les autres représentants ont présenté plus de 21 discours portant sur des enjeux ayant des répercussions sur la protection des renseignements personnels tels que des initiatives en matière de sécurité et la prestation de soins de santé.

Discours et événements spéciaux

Sensibilisation du grand public et communications

Le Commissariat à la protection de la vie privée du Canada est chargé, en vertu de la *LPRPDE*, d'élaborer et d'entreprendre des programmes d'information afin que le public et les organisations comprennent et reconnaissent davantage les règles qui régissent la collecte, l'utilisation et la communication des renseignements personnels. Bien qu'aucun mandat législatif de sensibilisation du grand public ne soit spécifié aux termes de la *Loi sur la protection des renseignements personnels*, le Commissariat a bel et bien le mandat de s'assurer que les ministères et organismes sont tenus responsables de leurs pratiques en matière de traitement des renseignements personnels. Il s'avère souvent nécessaire d'informer le public, ainsi que les ministères et les organismes, des exigences de la Loi et des politiques connexes ainsi que des répercussions des initiatives du gouvernement, courantes ou proposées, sur le droit à la vie privée des

Canadiennes et des Canadiens.

En 2004-2005, le Commissariat a entrepris un projet de planification stratégique des communications avec l'expertise de consultants externes; cela a donné lieu à une stratégie exhaustive en matière de communications et d'information pour les prochains exercices. Cette stratégie permettra au Commissariat d'adopter une approche plus globale et plus proactive de la planification et de la prestation des activités de communications, une approche des communications se rapportant à la *LPRPDE* davantage axée sur la sensibilisation du grand public afin de mieux faire connaître le Commissariat et les principaux enjeux en matière de protection de la vie privée conformément aux deux lois.

En plus de l'élaboration de cette stratégie, le Commissariat a entrepris les activités de communications suivantes en 2004-2005 :

peut pas aider le plaignant. Manifestement, il s'agit là d'une question importante qui devrait être traitée lors de la réforme de la *Loi sur la protection des renseignements personnels*.

Brian Murdoch c. Gendarmerie royale du Canada et commissaire à la protection de la vie privée du Canada
N^{os} de dossier de la Cour fédérale T-1180-04 et de la Cour d'appel fédérale A-183-05

M. Murdoch a porté plainte à la commissaire à la protection de la vie privée, accusant la GRC d'avoir enfreint, entre autres comportements fautifs, la *Loi sur la protection des renseignements personnels* en communiquant ses renseignements personnels à son employeur sans son consentement. Le commissaire adjoint chargé de la *Loi sur la protection des renseignements personnels* a convenu que cette plainte relative à la communication était fondée.

Le 18 juin 2004, M. Murdoch a sollicité une révision judiciaire du rapport du commissaire adjoint sur sa plainte relative à la communication. Bien que la *Loi sur la protection des renseignements personnels* limite les recours aux questions d'accès, M. Murdoch a fait valoir que la commissaire à la protection de la vie privée doit nécessairement être habilitée à formuler des ordonnances remédiatrices et des redressements dans les cas (comme le sien) où la *Loi* a été transgressée.

Le 29 juin 2004, la commissaire à la protection de la vie privée a contesté la requête de M. Murdoch voulant qu'elle produise une copie authentifiée de tous les documents pertinents en sa possession. En août 2004, elle a déposé une requête en radiation de la demande. Cependant, le tribunal a refusé la motion en septembre 2004 en soulignant que le bien-fondé de l'argument de la commissaire à la protection de la vie privée (selon lequel elle n'a pas le pouvoir ou la compétence d'accorder les réparations demandées) pourrait facilement être déterminé lorsque le tribunal entendrait la requête.

Lors d'une audience tenue en mars 2005, le tribunal a déterminé que la commissaire à la protection de la vie privée avait rempli ses obligations en vertu de la *Loi sur la protection des renseignements personnels* et qu'elle avait correctement informé le requérant que la *Loi* ne prévoit aucune pénalité pour l'atteinte à la vie privée du requérant. Celui-ci ne peut obtenir du tribunal aucune autre indemnité pour la communication inappropriée.

M. Murdoch a interjeté appel de la décision de la Cour fédérale en avril 2005.

Mamidié Keita et Bernard Michaud c. ministre de l'Immigration du Canada et commissaire à la protection de la vie privée du Canada
N° de dossier de la Cour fédérale T-676-03

Les plaignants avaient demandé des renseignements personnels à tous les bureaux de Citoyenneté et Immigration Canada (CIC), particulièrement aux ambassades situées en Guinée, en Côte d'Ivoire, au Ghana et au Sénégal. Insatisfaits de la réponse de CIC, ils ont porté plainte au commissaire à la protection de la vie privée, qui a fait enquête et conclu que la plainte était fondée au moment où elle avait été déposée. Cependant, puisque CIC a communiqué aux plaignants des renseignements supplémentaires auxquels ils avaient droit au cours de l'enquête, le commissaire à la protection de la vie privée a conclu que la plainte était résolue. Le commissaire partageait l'avis de CIC selon lequel le reste des renseignements dont la communication a été refusée aux plaignants étaient des renseignements relatifs à un tiers faisant l'objet d'une exemption aux termes de l'article 26 de la *Loi sur la protection des renseignements personnels*.

Les plaignants ont alors déposé un recours en révision en vertu de l'article 41 de la *Loi sur la protection des renseignements personnels*. Puisque le recours cite à tort le commissaire à la protection de la vie privée à titre d'intimé, le commissaire à la protection de la vie privée par interim a déposé une motion en juillet 2003 afin d'être exclu du recours. Le tribunal a rejeté la motion en laissant entendre que la question dans ce dossier était trop complexe et qu'il était préférable de trancher celle-ci à l'instruction.

Le 28 avril 2004, le recours a été rejeté et le tribunal réitérait que les requérants ne peuvent pas, au moyen d'un recours en révision contre l'institution gouvernementale, également obtenir une révision judiciaire des recommandations du commissaire. Par ailleurs, le tribunal a confirmé que les exemptions de l'article 26 étaient appropriées et que les requérants avaient reçu tous les renseignements auxquels ils avaient droit.

Révision judiciaire

Les requérants sollicitèrent parfois, en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*, une révision judiciaire de la décision de la commissaire à la protection de la vie privée. Cela est produit dans le cas décrit ci-dessous, alors que la commissaire a dû expliquer sa compétence au tribunal lorsque le plaignant a tenté d'obtenir des réparations que la commissaire n'avait pas le pouvoir d'accorder. Ce cas illustre les recours sérieusement limités prévus en vertu de la *Loi sur la protection des renseignements personnels* pour toute infraction autre que les refus d'accès inappropriés. La commissaire se trouve dans la position peu enviable d'avoir à démontrer au tribunal qu'elle ne

redressement qui n'est pas disponible. Voici deux de ces cas qui ont fait l'objet d'une décision au cours de l'exercice :

Gauthier c. Canada (ministère de la Justice) et commissaire à la protection de la vie privée du Canada
N° de dossier de la Cour fédérale T-653-02

M. Gauthier a demandé que le ministre de la Justice lui donne accès à tous les renseignements personnels le concernant. Après avoir consulté plusieurs autres institutions, le Ministère lui a fait parvenir un total de 685 pages d'information et l'a avisé que certains renseignements n'avaient pas été communiqués conformément aux articles 26 et 27 de la *Loi sur la protection des renseignements personnels*. M. Gauthier a porté plainte au commissaire à la protection de la vie privée, accusant le Ministère de lui refuser indûment la communication de ses renseignements personnels.

L'ancien commissaire à la protection de la vie privée a examiné les renseignements dont la communication avait été refusée, et il a convenu que les exceptions prévues aux articles 26 et 27 avaient été appliquées adéquatement et que, par conséquent, la plainte était non fondée. Néanmoins, le commissaire a demandé au ministre de la Justice de revoir sa position quant à l'exercice de son pouvoir discrétionnaire en ce qui concerne certains renseignements, à la suite de quoi les renseignements ont été communiqués à M. Gauthier.

M. Gauthier a déposé un recours en vertu de l'article 41 de la *Loi sur la protection des renseignements personnels*, dans lequel il demandait indûment, entre autres choses, la révision des conclusions du commissaire à la protection de la vie privée concernant sa plainte.

En octobre 2003, le commissaire à la protection de la vie privée par intérim a présenté ses observations sur le manque de compétence des tribunaux à l'égard de la révision des conclusions du commissaire à la protection de la vie privée.

Au cours d'une audience tenue le 31 mars 2004, M. Gauthier a concédé qu'en fait il ne cherchait pas une révision des conclusions du commissaire à la protection de la vie privée, mais seulement de la décision de l'institution gouvernementale de refuser de lui donner accès à tous les renseignements personnels le concernant. Dans une décision qui a donné lieu à un examen des principes du secret professionnel, le recours contre le gouvernement a été accueilli en partie le 4 mai 2004.

Recours judiciaires en vertu de la Loi sur la protection des renseignements personnels

Selon l'article 41 de la *Loi sur la protection des renseignements personnels*, une personne est autorisée, à l'issue d'une enquête de la commissaire à la protection de la vie privée, à déposer auprès de la Cour fédérale du Canada un recours en révision du refus du gouvernement de lui communiquer ses renseignements personnels. Les recours suivants ont été déposés au cours du dernier exercice :

1. Keith Maydak c. Solliciteur général du Canada (N° de dossier de la Cour fédérale T-972-04)
2. James R. Gairdner c. Jennifer Stoddart et autres (N° de dossier de la Cour fédérale T-2005-04) Requête abandonnée en février 2005

En vertu de l'article 42 de la *Loi sur la protection des renseignements personnels*, la commissaire à la protection de la vie privée est autorisée à comparaître devant la Cour fédérale. Elle peut déposer auprès de la Cour fédérale un recours en révision de la décision d'une institution qui a refusé de communiquer des renseignements personnels (avec le consentement du plaignant). Elle peut également comparaître devant la Cour au nom de la personne qui a exercé un recours devant elle, ou comparaître, avec l'autorisation de la Cour, comme partie à une instance engagée en vertu de l'article 41. Au cours du dernier exercice, aucune de ces possibilités n'a nécessité la présence en cour de la commissaire à la protection de la vie privée.

La commissaire à la protection de la vie privée peut également participer à des recours lorsque le plaignant la désigne à tort à titre d'intimée et qu'il tente d'obtenir d'elle un

- acquérir les compétences nécessaires pour effectuer les EFVP ;
- coordonner et intégrer la contribution des intervenants ;
- documenter les observations à l'aide des éléments nécessaires ;
- concilier les EFVP et d'autres politiques gouvernementales telles que celles concernant la sécurité gouvernementale, le couplage des données et le numéro d'assurance sociale ; et
- s'assurer que le public a accès aux résumés des EFVP.

L'étude conclut aussi que le rôle du Commissariat en matière de surveillance et de prestation de conseils est crucial pour s'assurer de l'intégrité du processus d'évaluation ainsi que de la confiance du public à l'égard de la politique. Nous sommes heureux que l'étude reconnaisse la nécessité de se procurer les ressources financières adéquates. Ce sujet fera partie d'une analyse globale de rentabilisation en vue du financement permanent du Commissariat qui sera soumise au Conseil du Trésor plus tard au cours de l'année 2005.

L'étude du Conseil du Trésor a également conclu qu'il n'existait aucune source d'information fiable indiquant le nombre d'évaluations qui avaient été menées. Et aucun mécanisme suffisamment efficace n'est en place pour s'assurer que les évaluations sont menées en vertu d'initiatives qui justifient une telle analyse. Les ministères se doivent d'améliorer leurs activités de contrôle et d'établissement des rapports, et le rapport annuel semble s'imposer comme méthode appropriée.

Au mois d'avril 2005, le Conseil du Trésor a fait part des lignes directrices révisées pour l'établissement des rapports pour l'exercice 2004-2005 en regard des rapports annuels concernant la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*. Nous sommes satisfaits de savoir que, selon ces lignes directrices, les ministères sont maintenant tenus de présenter un rapport sur le nombre d'EFVP et d'évaluations préliminaires effectuées au cours d'un exercice.

Compte tenu des faiblesses indiquées, nous envisageons de procéder à la vérification du fonctionnement de l'ensemble du système d'EFVP. Nous entretenons des inquiétudes à savoir si les évaluations sont effectuées lorsqu'elles le devraient. Il nous faut déterminer si les systèmes et procédures fonctionnent en vue d'assurer que les ministères prennent en charge les conclusions des évaluations en accord avec leur cadre ou leur programme de gestion de la vie privée.

personnel en ce qui a trait à son adhésion aux exigences de la politique. Ceux-ci sont aussi responsables de surveiller la mise en application des exigences.

Nous continuons à encourager les ministères à mettre sur pied une structure administrative officielle qui permettra d'examiner les initiatives ministérielles afin de déterminer s'il faut procéder à des EFVP. La structure ou les groupes devraient définir la responsabilité de l'émission de directives ministérielles et de lignes directrices sur la conformité aux objectifs de la politique, et mettre en place des groupes de gestion des EFVP. Ces groupes examinent les propositions afin de déterminer si les évaluations sont nécessaires, surveillent et coordonnent leur exécution, consultent les intervenants adéquats, approuvent les recommandations et suivent de près la mise en œuvre des recommandations.

Les ministères devraient également consulter les guides de vérification du Conseil du Trésor, en particulier la section du guide de vérification des EFVP intitulée « Cadre de contrôle de gestion » qui présente les structures administratives appropriées en appui à la politique.

Le processus d'examen des EFVP (tel que l'exige la politique du Conseil du Trésor) requiert que nous demandions de façon routinière aux ministères d'établir un rapport des mesures qui seront prises en réaction à nos recommandations. Nous évaluerons la conformité aux exigences et aux objectifs de la politique lors de toute vérification ultérieure.

Le Conseil du Trésor prévoit un examen complet de la politique d'EFVP en mai 2007, soit cinq ans après son lancement officiel. Toutefois, le Conseil a pris l'initiative en juin 2004 d'effectuer un examen intermédiaire d'un petit échantillon de ministères fédéraux et de programmes. Ainsi, le Conseil peut évaluer les répercussions sur la conformité en matière de protection des renseignements personnels, et déterminer les améliorations possibles. Au cours de l'examen, le Conseil a consulté les intervenants appropriés (dont le Commissariat). Nous sommes d'accord avec la plupart des recommandations et des conclusions de l'étude.

Selon les conclusions de l'étude, la politique a eu pour effet d'accroître de façon considérable la conformité en matière de protection des renseignements personnels au sein des ministères choisis. Plusieurs points requièrent, bien entendu, une attention particulière. Par exemple :

laquelle il indiquait avoir pris des mesures pour réagir à nos préoccupations. Ces mesures comprennent de meilleures ententes écrites avec les agents contractuels visant la protection des renseignements personnels, la restriction de l'accès aux systèmes municipaux et provinciaux de récupération de renseignements judiciaires aux cas de nécessité absolue, la réitération de non-divuligation de renseignements personnels aux employés, et l'amélioration des formulaires de consentement.

Toutefois, compte tenu des quatre années qui se sont écoulées, de la controverse entourant le Programme et des nombreuses modifications qui ont suivi, dont les changements apportés à la *Loi sur les armes à feu*, il est temps de mettre à jour nos connaissances du Programme en vue de préparer une nouvelle vérification.

Évaluation des facteurs relatifs à la vie privée

Le Conseil du Trésor du Canada exige que les ministères et organismes fédéraux évaluent les facteurs relatifs à la vie privée (EFPV) de tous les nouveaux programmes et services gouvernementaux soulevant des questions en matière de protection des renseignements personnels. Des évaluations sont également requises lorsque des ministères apportent des changements significatifs aux programmes et services existants que nécessitent la collecte, l'utilisation ou la communication de renseignements personnels ou plus détaillés. Les ministères doivent également évaluer les nouvelles activités de couplage de données, la sous-traitance ou tout autre changement ayant de possibles répercussions sur la protection de la vie privée.

La politique d'EFPV du Conseil du Trésor est essentielle à la protection de la vie privée. De plus, en dépit du manque d'uniformité des évaluations des facteurs relatifs à la vie privée en ce qui concerne la qualité et l'exhaustivité, celles-ci se sont considérablement améliorées. Cette tendance s'est poursuivie au cours de la dernière année. Nous sommes particulièrement ravis de constater que les ministères incluent de plus en plus souvent des plans d'action à leur présentation relative à l'EFPV. C'est là un signe encourageant des effets escomptés de la politique d'EFPV : s'assurer que le gouvernement accorde à la protection de la vie privée une importance de premier plan dans la planification, l'élaboration et la mise en œuvre de programmes et de services.

La mise en œuvre d'une stratégie permettant de respecter les exigences de la politique d'EFPV est plus qu'un élément clé d'un cadre ministériel de gestion de la vie privée. La politique en soi encourage l'adoption d'une structure de gouvernance en matière de protection de la vie privée. Par exemple, les lignes directrices de la politique déterminent les responsabilités fondamentales d'un cadre de gestion de la vie privée. Elles indiquent qu'il incombe aux responsables des ministères de préciser les rôles du

tirer profit de leurs connaissances et de leur expérience afin de renforcer leur aptitude à évaluer les facteurs relatifs à la vie privée de toute forme de fusion ou de couplage de données.

Compte tenu de la taille et de la complexité des systèmes de RHDCC et de DSC qui contiennent une grande quantité de renseignements personnels, nous envisageons effectuer une vérification afin de déterminer si les cadres de gestion des renseignements personnels sont maintenus et continuent à fonctionner avec efficacité.

Couplage des données

En vertu de la Politique des données du Secrétaire du Conseil du Trésor du Canada, les ministères et organismes fédéraux sont tenus d'aviser le Commissariat de toute proposition de couplage de données. Cette exigence a pour but de permettre au Commissariat d'examiner les propositions et de formuler des observations.

Compte tenu du peu de propositions de couplage de données qui nous sont déclarées, nos préoccupations se rapportent moins à leur existence qu'au risque que le couplage de données ne soit pas déclaré et/ou qu'il se soustrait à la vérification. Selon les informations obtenues du Secrétaire du Conseil du Trésor, une certaine confusion régne au sein des ministères quant à la définition du couplage de données. Comme cette confusion contribuerait possiblement au faible taux de déclaration de cette activité, le SCT s'est mis à la tâche pour régler la situation. Nous partageons cette préoccupation et favorisons une définition claire et étudiée qui engloberait cette activité sous toutes ses formes, qu'elles se nomment couplage, fusion ou forage de données.

À l'heure actuelle, il est difficile de savoir si le gouvernement fédéral connaît toute l'étendue du « couplage de données » de renseignements personnels ayant cours, y compris les activités menées par des tiers travaillant sous contrat pour le gouvernement fédéral, et si ces tiers respectent les lois et les politiques et ont des pratiques adéquates en matière de gestion des renseignements personnels. Nous continuerons à suivre l'évolution de la situation de près et envisageons la possibilité de mener une future vérification dans ce domaine.

Examen de suivi du Programme canadien des armes à feu

Le Commissariat a entrepris l'examen du Programme canadien des armes à feu en 2001. Depuis, nous avons suivi l'évolution de la situation (voir les pages 49 et 50 du Rapport annuel au Parlement 2003-2004). À la suite des négociations continues visant à améliorer les pratiques, nous avons reçu l'an dernier une réponse favorable du nouveau ministre de la Sécurité publique et de la Protection civile Canada, dans

entrevues ont été menées avec des membres du personnel des directions et des unités opérationnelles régionales. Nous avons observé les agents des douanes s'acquitter de leurs tâches aux lignes d'inspection primaire et secondaire. L'équipe a également bénéficié d'une séance d'information sur les systèmes électroniques utilisés aux postes frontaliers terrestres et dans les aéroports pour déterminer si un voyageur/passager représente un risque.

Cette étape de la vérification a été complétée au début de l'exercice financier 2005. Le début de l'examen détaillé est prévu pour le mois de mai 2005 et le rapport de vérification sera terminé en janvier 2006.

Autres activités de vérification et d'examen

Examen des banques de données de RHDCC

Depuis 2001, le Commissariat a procédé à l'étude d'environ 60 propositions de couplage de données faites par Développement des ressources humaines Canada (maintenant appelé Ressources humaines et Développement social Canada – DSC). Ces examens sont obligatoires en vertu d'un protocole de gestion entré en vigueur en 2000 à la suite des préoccupations importantes concernant le Fichier longitudinal de la main-d'œuvre de DRHC (démantelé depuis). Le protocole régit toute recherche future ayant trait au couplage de données.

La qualité des propositions de couplage de données soumises au Commissariat s'est considérablement améliorée – à un point tel que RHDCC sollicite rarement nos conseils. Le Ministère s'est doté des compétences requises à l'interne pour cibler les risques en matière de protection de la vie privée associés au couplage de données relié à la recherche et à l'évaluation des programmes et y réagir. Nous encourageons les autres ministères et organismes à adopter le protocole de gestion.

Par conséquent, le Commissariat a écrit, en mars 2005, aux deux ministères pour leur faire part de sa recommandation selon laquelle l'examen de leurs propositions de couplage de données pourrait être facultatif et effectué à la discrétion des ministères. Les ministères ont accepté la recommandation et apporteront les modifications appropriées au protocole de gestion. Nous avons proposé le changement sous réserve que les ministères maintiennent l'intégrité des structures et des procédures en place. Nous nous attendons en plus que DSC et RHDCC réduisent au minimum toute perturbation possible de l'examen interne causée par la séparation de leurs responsabilités. Finalement, nous encourageons le personnel des deux ministères à

Nous sommes d'avis que les objectifs en matière de sécurité nationale et de saines pratiques en matière de gestion des renseignements personnels sont interdépendants. Des contrôles rigoureux relativement à la collecte et à l'utilisation des renseignements personnels limiteront les risques d'atteinte à la protection de la vie privée, tels que l'utilisation ou la communication inappropriées, et soutiendront des objectifs rigoureux en matière de sécurité nationale. La communication, pertinente, opportune et exacte, des renseignements personnels est un principe vital aux opérations liées à l'application de la loi et au renseignement de sécurité. Toutefois, la communication doit avoir lieu selon les normes les plus élevées en matière de protection de la vie privée et de la sécurité, afin de conserver la crédibilité, auprès du public, des parlementaires et des partenaires étrangers.

Selon les critères généraux sous-tenant la vérification, la collecte, l'utilisation et la communication des renseignements personnels doivent se limiter aux renseignements nécessaires et permis par la loi. Il est également essentiel d'encadrer ces activités par de multiples mesures de protection de la vie privée et de la sécurité durant le cycle de vie des renseignements personnels afin de prévenir et d'atténuer les risques d'atteinte à la protection de la vie privée et aux objectifs des programmes.

Les programmes de l'ASFC en matière d'exécution des lois relatives aux douanes et à l'immigration supposent la collecte, l'utilisation et la communication d'une grande quantité de renseignements personnels de nature délicate. Les renseignements personnels recueillis comprennent des informations portant sur la situation financière, les antécédents familiaux, la santé et les voyages, des identificateurs personnels comme le numéro d'assurance sociale, les numéros d'immigration et de passeport, des éléments de biométrie – photos numériques, empreintes digitales et lecture de l'iris.

Compte tenu de la taille et de la complexité de l'ASFC, le Commissariat a utilisé la plupart de ses ressources limitées en matière de vérification pour déterminer lesquels des nombreux programmes et activités de gestion des renseignements personnels de l'Agence ont le plus de répercussions sur la vie privée des personnes. Voilà sur quoi se penchera le Commissariat au cours de la vérification.

Afin de mieux comprendre les activités de l'ASFC, l'équipe de vérificateurs a examiné les sources d'information ouvertes, les descriptions des activités de programme de l'ASFC, les politiques internes régissant la gestion des renseignements personnels, le matériel de formation pertinent, les diagrammes de circulation de l'information, les ententes sur l'échange de renseignements, les évaluations des facteurs relatifs à la vie privée et les descriptions des systèmes de technologie de l'information. Des

Security (DHS) des États-Unis ont travaillé à plusieurs initiatives d'utilisation de la technologie et des ressources afin de mieux gérer les risques à la frontière canado-américaine. Ces initiatives comprennent l'application conjointe de la loi, les centres de contrôle conjoints, des activités coordonnées du renseignement et des bases de données intégrées permettant l'échange de renseignements.

Toutefois, les Canadiennes et les Canadiens sont préoccupés par la circulation de renseignements personnels vers les États-Unis. Les médias ont révélé que les Canadiennes et les Canadiens ne sont pas disposés à renoncer à la protection de leur vie privée au profit de mesures qui n'améliorent pas clairement leur sécurité. C'est aussi ce que soutient un sondage commandé par le Commissariat aux Associations de recherche EKOS, selon lequel 75 p. 100 des Canadiennes et des Canadiens interrogés croient que les organismes gouvernementaux du Canada transfèrent les renseignements personnels des citoyens et des citoyens à des gouvernements étrangers dans le but de protéger la sécurité nationale et 85 p. 100 des répondants affirment qu'ils sont modérément ou très préoccupés par de tels transferts.

Les défenseurs de la protection de la vie privée et des droits de la personne ainsi que des politiciens canadiens ont tous fait part de leurs préoccupations face aux répercussions de la circulation transfrontière de données personnelles. Au nombre de ces préoccupations, l'exploration des données, l'établissement de profils raciaux, l'accès direct aux bases de données dont jouissent les autorités américaines, l'usage secondaire des renseignements personnels, le couplage des données et des renseignements personnels que détient le secteur privé, et la possibilité que la *USA PATRIOT Act* supplante le droit à la protection de la vie privée des Canadiennes et des Canadiens.

Compte tenu du contexte, le Commissariat a avisé, en juillet 2004, le président de l'Agence des services frontaliers du Canada (ASFC) qu'il avait l'intention d'effectuer la vérification de la gestion que fait l'Agence de la circulation transfrontalière des renseignements personnels qui sont sous son autorité.

L'objectif de la vérification est d'évaluer la mesure dans laquelle l'ASFC contrôle et protège adéquatement la circulation des renseignements personnels des Canadiennes et des Canadiens vers des gouvernements étrangers ou vers leurs institutions. La vérification se concentrera sur l'échange de renseignements personnels entre le Canada et les États-Unis. Un des éléments clés consistera à établir une correspondance (dans la mesure du possible) entre les renseignements personnels des Canadiennes et des Canadiens que l'ASFC communique aux États-Unis et les fins visées par cette communication.

Il faudra un certain temps pour mettre en place des mesures de vérification suffisantes, en plus de répondre à la demande des ministères pour des examens en temps opportun des évaluations des facteurs relatifs à la vie privée, comme l'exige la politique du Conseil du Trésor. Pour ce faire, nous avons entrepris les démarches suivantes :

- l'achèvement de méthodes et de pratiques d'examen et de vérification externes ;
- la définition du but de la Direction et l'articulation de l'institution/organisme autour des valeurs prônant le travail d'équipe ;
- l'amorce d'un processus visant à élaborer une stratégie et un plan de vérification à plus long terme compte tenu des risques et des enjeux relatifs à la protection des renseignements personnels ;
- l'élaboration d'une analyse de rentabilisation qui sera présentée au Conseil du Trésor du Canada afin d'obtenir davantage de financement pour la vérification et l'examen ;
- la sensibilisation auprès des comités parlementaires en ce qui touche les vérifications en matière de protection des renseignements personnels ; et
- l'amélioration des pratiques de vérification dans le cadre de la vérification de l'Agence des services frontaliers du Canada (voir ci-bas).

Vérification de la circulation transfrontalière des renseignements personnels

Tel qu'il a été mentionné plus tôt dans ce rapport, l'amélioration de la sécurité aux frontières est devenue, depuis les événements du 11 septembre 2001, une priorité pour le Canada et les États-Unis. De nombreuses mesures de sécurité nationale ont été présentées en vertu de la Déclaration Manley/Ridge sur la frontière intelligente, émise en décembre 2001, et du plan d'action en 30 points.

Depuis, le gouvernement a alloué environ 10 milliards de dollars aux programmes et initiatives touchant la sécurité nationale. Sur ce montant, plus de 1,7 milliard de dollars ont été accordés à l'Agence des services frontaliers du Canada (ASFC) dans le but de mettre en œuvre des mesures visant à renforcer les infrastructures terrestres et maritimes ainsi que celles des aéroports et des postes frontaliers, et visant à augmenter les ressources humaines de l'Agence et à améliorer ses outils de détection.

Le Canada et les États-Unis se sont aussi engagés à améliorer l'application de la loi aux frontières en étudiant les options qui s'offrent pour échanger des renseignements et faire un meilleur usage de la technologie. L'ASFC et le *Department of Homeland*

Vérification et examen

Renforcer la fonction de vérification

La Loi sur la protection des renseignements personnels confère à la commissaire à la protection de la vie privée (paragraphe 37(1)) l'autorité de mener des enquêtes sur l'application que quelque 150 institutions gouvernementales font des articles 4 à 8 de la Loi. Ces articles régissent la manière dont le gouvernement fédéral recueille, conserve, détruit et protège les renseignements personnels. La Loi autorise également la commissaire à effectuer la vérification de certaines banques de données soustraites à l'accès.

En mars 2005, le Commissariat a donné à la Direction de l'examen de la conformité le nom de Direction de la vérification et de la revue. Cela témoigne d'un changement important. Le Commissariat n'a pas utilisé ses pleins pouvoirs de vérification pour évaluer la qualité de la gestion en matière de protection des renseignements personnels, ni pour aborder les risques qui y sont inhérents dans les activités actuelles du gouvernement fédéral. Au cours de la dernière année, nous avons entrepris de reconstituer et de renforcer les fonctions de vérification et d'examen. Nous avons l'intention de recourir plus souvent à la vérification, laquelle deviendra un outil important qui nous permettra de remplir notre mandat en vertu de la Loi sur la protection des renseignements personnels et de la LPPDE.

L'objectif du Commissariat consiste à « procéder de façon objective et indépendante à la vérification et à l'examen de systèmes de gestion de renseignements personnels dans le but de promouvoir la conformité aux lois en vigueur, aux politiques et aux normes et d'améliorer les pratiques en matière de protection de la vie privée et d'imputabilité ».

souvent posées par le public, dont celles concernant le vol d'identité, le télémarketing et, bien entendu, le numéro d'assurance sociale. Nous continuons également à ajouter des renseignements sur notre site Internet afin de répondre aux questions les plus fréquentes. Nous avons aussi assigné quelques enquêteurs à l'Unité des requêtes et renseignements afin qu'ils prêtent assistance à cette dernière. Finalement, nous invitons désormais les personnes à nous téléphoner pendant les heures de bureau puisqu'il est souvent plus rapide et plus facile pour nous de cerner ainsi leurs besoins plutôt que par une série de lettres ou de courriels.

STATISTIQUES SUR LES DEMANDES DE RENSEIGNEMENTS

(du 1^{er} avril 2004 au 31 mars 2005)

Le tableau ci-dessous indique le nombre total de demandes de renseignements en vertu de la Loi sur la protection des renseignements personnels auxquelles l'Unité des requêtes et renseignements a répondu.

2 391	Demandes de renseignements reçues par téléphone
585	Demandes de renseignements reçues par écrit (courrier, courriel et télécopieur)
2 976	Nombre total de demandes de renseignements reçues

Délais d'exécution des demandes de renseignements

Le Commissariat reçoit 80 p. 100 des demandes de renseignements par téléphone. La plupart d'entre elles sont traitées immédiatement ; les autres, qui peuvent nécessiter de la recherche, sont traitées au cours des deux semaines subséquentes.

Les demandes de renseignements envoyées par écrit représentent 20 p. 100 de la charge de travail et elles étaient traitées en moyenne au cours des trois mois suivants. Fournir des réponses écrites aux demandes de renseignements exige parfois beaucoup de temps et un travail intense. Au cours de l'année, l'Unité des requêtes et renseignements a encouru des arriérés relatifs aux demandes de renseignements écrites, ce qui a eu pour effet de repousser au maximum les délais d'exécution mensuels moyens. Au cours du prochain exercice financier, nous prévoyons mettre en œuvre de nouvelles mesures et obtenir des ressources additionnelles afin de traiter plus rapidement les requêtes du public.

qu'on prévienne communiquer plus de renseignements personnels qu'il n'est nécessaire pour aborder une question d'intérêt public. Ainsi, l'immixtion dans la vie privée d'une personne est réduite au minimum.

L'an dernier, nous avons examiné 76 de ces avis, dont un grand nombre se retrouve dans deux catégories. Dans la première, il était question de communiquer les circonstances de la mort d'une personne aux membres de la famille. Nous avons reçu 24 avis de ce type ; la plupart provenaient du Service correctionnel du Canada (SCC) et du ministère de la Défense nationale.

Le second groupe d'importance considérable – 21 avis – provenait de la Gendarmerie royale du Canada (GRC) et du SCC et concernait des personnes illégalement en liberté ou libérée de leur lieu de détention à la fin de leur peine. Toutes ces personnes sont à risque de récidiver et représentent donc un danger pour la communauté.

Un autre groupe de 11 avis traitait de communication de renseignements à des comités parlementaires, des commissions d'enquête ou d'autres entités publiques se rapportant à des sujets tels que le programme des commandites, des allégations d'inconduite par des fonctionnaires ou les circonstances entourant des morts accidentelles.

Il est aussi digne d'intérêt de signaler quatre avis de Santé Canada concernant des personnes atteintes de maladies transmissibles posant un risque pour la santé publique, deux avis de la Société d'aide à l'enfance concernant des mauvais traitements présumés sur des enfants et quatre avis de menace pour la sécurité.

Demandes de renseignements

L'Unité des requêtes et renseignements traite les demandes de renseignements du public en vertu de la Loi sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels et les documents électroniques. Pour l'année sur laquelle porte ce rapport, l'Unité a traité près de 3 000 demandes de renseignements concernant des questions relevant de la Loi sur la protection des renseignements personnels et quelque 17 000 au titre de la Loi sur la protection des renseignements personnels et les documents électroniques. Au cours de l'année, la pénurie d'effectifs à l'Unité des requêtes et renseignements, associée à la charge de travail élevée en permanence, nous ont occasionné des problèmes. Résultat : il nous a fallu modifier notre façon de donner suite aux demandes de renseignements du grand public. Nous n'acceptons plus les demandes de renseignements ou les plaintes reçues par courriel. Nous avons instauré un système téléphonique automatisé pour répondre aux questions les plus

L'alinéa 8(2)m) de la *Loi sur la protection des renseignements personnels* accorde aux responsables d'institutions fédérales le pouvoir discrétionnaire de communiquer des renseignements personnels sans obtenir le consentement de la personne concernée lorsque celle-ci en tirerait un avantage certain ou lorsque des raisons impérieuses d'intérêt public l'emportent sur une éventuelle atteinte à la vie privée. La personne responsable de l'institution est tenue (en vertu du paragraphe 8(5)) de donner un préavis écrit de la communication des renseignements personnels à la commissaire à la protection de la vie privée, de préférence à l'avance (à moins qu'une situation urgente ne justifie le contraire). Le Commissariat examine ces cas de communication et, si cela est jugé nécessaire, la commissaire à la protection de la vie privée avise les personnes auxquelles se rapportent les renseignements personnels. Au cours du processus d'examen, le Commissariat émet également des avis aux institutions lorsqu'il semble

Communication dans l'intérêt du public en vertu de la Loi sur la protection des renseignements personnels

La « Photographique » est de nouveau présente sur le site, et elle ne contient aucune photo d'employés. *Entre nous* a aussi été réintégré au site du SCC, et toutes les personnes sur les photos ont signé un formulaire de consentement et de renonciation de droits.

Après avoir été contactée par le SCC, la CBC a retiré les photographies offensantes de son site. Le SCC a également retiré les photos controversées de la « Photographique ». Le SCC a par la suite examiné chacune des photos restantes et s'est assuré que chaque personne avait signé une renonciation de droits avant que leurs photos ne soient affichées sur le site. Toutefois, le SCC a reconnu que le libellé de la renonciation de droits devait être mis à jour afin de s'assurer que les employés aient compris qu'une fois leurs photos affichées sur le site Internet, elles pouvaient être reproduites et utilisées à des fins autres que des articles à propos du SCC. Le Ministère a entrepris de longs pourparlers auprès de la direction et des services juridiques au sujet du consentement des employés. Le SCC a également retiré temporairement *Entre nous* du site, jusqu'à ce que toute la question soit réglée.

Dans le cas qui nous occupe, la CBC préparait un reportage sur des allégations de mauvais traitements à l'endroit des détenus par les agents de correction dans l'unité d'isolement du pénitencier de Kingston. La CBC s'est procuré une photographie d'un groupe d'agents de correction sur le site du SCC dont elle s'est servie pour illustrer l'article sur les mauvais traitements dans l'unité d'isolement. Bien que ces personnes ne soient pas rattachées à l'unité en question, la CBC, en utilisant la photo dans ce contexte, a laissé croire le contraire.

revenu sous le pont *False Creek Bridge*. Le sac contenait 12 paquets de bordereaux de paiement d'impôt provenant de deux établissements financiers. Sur les bordereaux étaient inscrits le nom, l'adresse, le montant du paiement et le numéro de compte de plusieurs personnes et entreprises. Seulement deux paquets avaient été ouverts, et tous les documents étaient trempés et exposés aux intempéries depuis un certain temps. Ces renseignements avaient été traités directement par un organisme de compensation privé travaillant à contrat pour les deux établissements financiers en question. On présume que le sac avait été volé lors de son transport entre les établissements financiers et l'Agence du revenu du Canada.

Au moment du vol, l'Agence a établi que le sac volé contenait 1 600 bordereaux de paiement. Si la majorité des bordereaux se rapportaient à des entreprises, 390 d'entre eux concernaient des personnes. Puisque l'organisme de compensation ne prévoyait pas communiquer avec les personnes concernées, l'Agence a, de sa propre initiative, avisé les clients afin qu'ils puissent prendre des mesures pour prévenir le vol d'identité. Le Commissariat confirme que les clients ont effectivement été informés de la situation au moment du vol. Tous les renseignements ont vraisemblablement été retrouvés et aucune plainte individuelle en matière de protection de la vie privée n'a été reçue relativement à ce vol. La commissaire à la protection de la vie privée a transmis ses félicitations à l'Agence pour l'initiative qu'a prise celle-ci afin de protéger les renseignements personnels de ses clients, bien qu'elle n'était pas responsable de cette atteinte à la protection de la vie privée.

Des photos d'employés du SCC accompagnent un reportage du réseau anglais de la CBC

Un agent de correction du Service correctionnel du Canada (SCC) a rapporté que le 16 novembre 2004, il avait vu une photo de lui et de certains de ses collègues sur un site Internet de la CBC, accompagnant un texte intitulé « *Un ombudsman se penche sur des allégations de mauvais traitement dans un établissement carcéral* » [traduction].

Sur le site Internet du SCC, on retrouve une « Photothèque » contenant diverses photographies de pénitenciers, d'édifices à bureaux du SCC et d'agents de correction au travail. Les photos sont destinées aux médias afin d'illustrer des articles. On retrouve aussi une publication à l'intention des employés intitulée *Entre nous* [traduction] sur le site Internet du SCC – elle est donc accessible au public – la publication renferme souvent des photographies d'employés au travail.

Deux éléments ont contribué à la communication inappropriée : la surveillance s'est méprise sur le processus de contrôle d'accès du système – la communication n'était pas intentionnelle – et le CGD n'a pas réussi à classifier adéquatement le message avant de le rendre accessible sur le système.

Depuis la plainte, Statistique Canada a transmis à tout le bureau des directives quant à l'attribution d'un niveau de sécurité aux courriels. L'organisme étudie aussi la possibilité que le personnel du CGD examine tous les courriels Outlook qui arborent un indicateur désignant un niveau de sécurité avant de l'intégrer à la base de données. À plus long terme, Statistique Canada examinera le fonctionnement du CGD ainsi que ses protocoles en matière de renseignements personnels et présentera au Commissariat un rapport sur le progrès accompli.

Le Commissariat a conclu que la plainte était fondée mais, compte tenu du travail en cours pour améliorer le système de courrier électronique, il n'engagera pas d'autres mesures afférentes.

Incidents en vertu de la Loi sur la protection des renseignements personnels

Outre les plaintes individuelles, nous procédons à des enquêtes sur des incidents relatifs à la collecte, à l'utilisation ou à la communication inappropriée de renseignements personnels qui sont portés à l'attention du Commissariat par diverses sources dont les médias, et par les ministères eux-mêmes. Ces enquêtes font souvent ressortir des problèmes institutionnels ou des violations non reconnues en matière de protection de la vie privée qui nécessitent un redressement dans des délais les plus courts possibles. L'an dernier, le Commissariat a mené et terminé 27 enquêtes concernant la mauvaise gestion de renseignements personnels. Sur les 27 enquêtes, cinq se rapportaient à des renseignements personnels acheminés à la mauvaise personne. Ces cinq cas se sont révélés être des incidents isolés et ont incité les employés de l'État à faire preuve d'une vigilance accrue.

Deux de ces cas sont décrits ci-dessous.

Un jardinier trouve des renseignements relatifs à l'impôt sur le revenu

Plusieurs incidents concernaient des renseignements volés. Par exemple, un jardinier à l'emploi de la Commission des parcs de Vancouver a trouvé, au début de l'année 2004, un sac contenant des renseignements relatifs à l'impôt sur le

Un système de courrier électronique déconcerte le destinataire et laisse transparente des inquiétudes en matière de sécurité

Un employé de Statistique Canada s'est plaint qu'un courriel de sa superviseuse, dans lequel cette dernière le qualifiait de violent et affirmait qu'il menaçait la sécurité d'autrui, constituait une utilisation et une communication inappropriées de ses renseignements personnels. Tout le personnel a accès aux courriels échangés entre la superviseuse et un agent des ressources humaines via le réseau interne de l'organisme et ce, pendant cinq semaines.

Le plaignant avait déposé une plainte pour harcèlement contre sa superviseuse. Dans le courriel, la superviseuse se disait préoccupée par la possibilité que l'employé reçoive des copies de sa déclaration de témoin ou de celle d'autres employés concernant la plainte pour harcèlement.

Statistique Canada a mené une enquête en regard de la plainte, envisageant la possibilité d'une violation à la fois de la sécurité interne et des politiques en matière de protection des renseignements personnels. Le système de courrier électronique de l'organisme permet aux usagers d'indiquer la nature de leurs courriels : normal, personnel, privé ou confidentiel. Toutefois, le Centre de gestion des documents (CGD), qui administre et entretient les systèmes de communication électronique, ne capte pas toujours cet indicateur.

Le courriel faisant l'objet du litige a été envoyé via le CGD en se servant de l'option de messagerie du bureau, laquelle permet d'envoyer ou de choisir une des deux autres possibilités d'envoi en sélectionnant la fonction « Options ». Le destinataire peut choisir l'option « Accessibilité » qui lui permet de déterminer le niveau de sécurité et de diffusion du message, ou l'option « Accès restreint » qui permet l'accès en mode « lecture seule ». Le destinataire peut également aviser le CGD du niveau d'accessibilité souhaité. Toutefois, il ne sera au courant des choix offerts qu'après avoir sélectionné la fonction « Options ».

La superviseuse avait tenté de classifier son message en inscrivant par Microsoft Outlook l'indicateur « privé » ou « confidentiel ». Elle n'avait pas compris qu'elle aurait du également inscrire l'indicateur « protégé » à l'intention du CGD. Selon sa procédure, le CGD demande à ses classificateurs de vérifier les renseignements dans l'en-tête, d'en étudier le contenu, de vérifier le niveau de sécurité et, si ce dernier n'est pas clair, de le confirmer auprès du destinataire. Le message est ensuite acheminé aux destinataires appropriés.

renseignements. L'enquêteur a également étudié un document de TPSCG expliquant les raisons pour lesquelles les renseignements étaient requis. Par la suite, le service a accepté, à la demande de l'enquêteur, d'omettre la date de naissance et de laisser le choix d'inscrire ou non les noms des répondants en cas d'urgence et le numéro de téléphone à la maison.

Le plaignant a examiné le formulaire révisé du profil du voyageur et s'est montré satisfait qu'on ne demande plus la date de naissance et que la déclaration d'autres renseignements soit désormais facultative. Les explications données par le service au sujet des mesures de protection des renseignements ont également satisfait le plaignant ; celui-ci a consenti à considérer la plainte comme réglée en cours d'enquête.

L'achat d'un billet d'exposition n'est pas une invitation à des activités de marketing

Une amatrice d'art qui s'était procuré un billet pour l'exposition Klimt au Musée des beaux-arts du Canada est restée stupéfaite lorsqu'on l'a sollicitée pour soutenir les programmes réguliers du Musée. Peu de temps après avoir acheté le billet pour l'exposition Klimt, la plaignante a reçu un appel de la Fondation du Musée des beaux-arts du Canada lui demandant si elle avait apprécié l'exposition. Elle a mis fin à l'appel.

Quelque temps plus tard, lorsqu'un bénévole de la Fondation lui a téléphoné de nouveau pour lui demander son appui, la plaignante a voulu savoir comment il savait qu'elle avait visité le musée et comment il se faisait qu'elle était sur la liste d'appels. Puisque le bénévole l'ignorait, elle s'est informée directement au musée, où on lui a appris que le musée communiquait couramment à la Fondation, aux fins de collecte de fonds, les renseignements personnels des gens qui avaient acheté des billets.

La femme a porté plainte pour communication inappropriée de renseignements auprès de la commissaire à la protection de la vie privée. L'enquêteur a confirmé que le musée se constituait une base de données à partir des ventes de billets, à l'usage des campagnes d'adhésion et pour promouvoir les expositions futures. Le musée a fait supprimer le nom de la plaignante de la base de données et a présenté ses excuses pour les appels. Il s'est engagé également à obtenir dorénavant le consentement exprès des gens qui se sont procurés des billets avant d'ajouter leur nom à la base de données.

La plaignante s'est montrée satisfaite de l'issue de la plainte et le Commissariat estime celle-ci réglée en cours d'enquête.

La comptable a aussi indiqué qu'à l'exception de la date de naissance, tous les renseignements requis pour accéder en direct sont inscrits sur l'avis de cotisation. Puisqu'un contribuable se voit souvent demander son avis de cotisation à titre de preuve de revenu par des prêteurs, fournisseurs de cartes de crédit, conseillers financiers et autres institutions, n'importe qui ayant une copie de l'avis peut accéder au dossier du contribuable. La plaignante n'était pas en mesure de prouver que des accès non autorisés avaient eu lieu.

Le Commissariat a conclu que les mesures de sécurité prises par l'ARC étaient suffisantes pour protéger les renseignements personnels des contribuables contenus dans le système et que la plainte était non fondée. De plus, la *Loi de l'impôt sur le revenu* oblige l'ARC à fournir un avis de cotisation aux contribuables. Dès lors où le contribuable est en possession de l'avis, la responsabilité de la protection de ses renseignements personnels lui incombe.

Création d'un profil du voyageur pour les fonctionnaires

Un employé de l'État s'est plaint de la quantité de renseignements personnels que Travaux publics et Services gouvernementaux Canada (TPSGC) recueille par le biais du formulaire Profil des voyageurs.

Le gouvernement fédéral a complètement réorganisé sa façon d'effectuer les préparatifs de voyage pour ses employés. Il a créé le Bureau de modernisation des services de voyage du gouvernement, lequel a par la suite octroyé par contrat à Accenture la responsabilité de fournir tous les services ayant trait aux voyages gouvernementaux. Par la suite, Accenture a sous-traité les services de cartes de crédit et de voyages à American Express.

Les employés de l'État doivent maintenant faire tous leurs préparatifs de voyage par l'entremise de Travel Access Voyage. Mais ils doivent d'abord remplir leur profil du voyageur en vue d'obtenir leur numéro d'identification du voyageur avant d'entreprendre des préparatifs de voyage. Le profil est envoyé à la compagnie de cartes de crédit qui émet ensuite le numéro.

Les renseignements requis comprennent les groupe et sous-groupe et le niveau du poste de l'employé, le numéro de téléphone à la maison ainsi que l'adresse domiciliaire des voyageurs, les noms de répondants en cas d'urgence, et la date de naissance. L'enquêteur a procédé à l'examen du formulaire et a rencontré le personnel de TPSGC afin de déterminer les raisons pour lesquelles les employés devaient fournir ces

deux documents sont délivrés selon des règles moins rigoureuses et peuvent être falsifiés. Le Bureau des passeports exige maintenant ces renseignements additionnels pour confirmer l'exactitude de la déclaration du demandeur et afin d'éviter la mise en circulation de faux passeports. Les demandeurs peuvent utiliser les passeports expirés à titre de preuve de citoyenneté canadienne, mais non comme pièce additionnelle d'identité.

Le Commissariat a conclu que le Bureau des passeports détenait l'autorité légale de recueillir des renseignements additionnels afin de confirmer l'identité du demandeur. L'objectif n'est pas d'imposer des restrictions draconiennes aux demandeurs, mais de permettre au Bureau des passeports de s'assurer de l'identité du détenteur et de préserver la sûreté du passeport canadien.

La plainte est considérée non fondée.

La sécurité en direct des renseignements personnels des contribuables

Une comptable agréée a remis en question la sûreté du système en direct de l'Agence du revenu du Canada (ARC). Elle s'est plainte que le système actuel puisse communiquer de façon inappropriée les renseignements personnels des contribuables. Les contribuables n'ont pas à demander l'accès en ligne, il est disponible par défaut. La plaignante affirme que l'ARC laisse aux contribuables la responsabilité de la protection de leurs renseignements. Elle ajoute que l'ARC devrait plutôt demander aux contribuables qui souhaitent obtenir le service en direct de s'enregistrer et devrait ensuite relever les normes de sécurité.

Au mois d'octobre 2003, l'ARC a instauré un programme permettant aux contribuables d'accéder aux renseignements relatifs à leur impôt pour les années 2001 et 2002, par la section « Mon dossier » du site Internet de l'ARC à l'adresse www.cra-arc.gc.ca. Pour y avoir accès, les contribuables doivent donner leur numéro d'assurance sociale, leur date de naissance, le montant de leur revenu indiqué à la ligne 150 et le code d'accès de huit chiffres indiqué sur leur avis de cotisation. Les contribuables peuvent bloquer l'accès en direct à leurs renseignements en téléphonant au Bureau d'aide des services électroniques pour les particuliers de l'ARC au numéro sans frais prévu à cet effet.

L'ARC protège également les renseignements par des mesures telles que les technologies de chiffrement et les mesures de sécurité. Les contribuables qui veulent utiliser le service doivent disposer d'un navigateur sécurisé, lequel requiert l'usage d'un mot de passe personnel assigné au contribuable.

Le plaignant refusait de fournir une carte santé, un permis d'armes à feu ou un permis de conduire comme preuve d'identité, en faisant valoir que les Canadiennes et les Canadiens ne sont pas légalement tenus de posséder ces documents et qu'exiger l'un d'eux constituait une violation de la *Charte* et de la *Loi sur la protection des renseignements personnels*. L'homme s'est également opposé à fournir l'adresse de son employeur ou d'un établissement d'enseignement qu'il aurait fréquenté au cours des deux dernières années parce qu'une telle exigence empêcherait de fait les personnes retraitées ou sans emploi d'obtenir un passeport.

En dernier lieu, l'homme a allégué qu'en demandant des références d'au moins deux personnes avec qui il n'avait aucun lien de parenté, le Bureau des passeports ajoutait une difficulté supplémentaire aux gens comme lui qui, à cause de problèmes de santé ou d'un handicap physique, avait des relations limitées. Il a également fait valoir que les membres de la famille ne devraient pas être automatiquement exclus à titre de référence.

L'enquêteur à la protection de la vie privée a rencontré le personnel du Bureau des passeports afin d'examiner les exigences. Le pouvoir de délivrance de passeports relève de l'exercice d'une prérogative royale, non d'une loi particulière. Le Bureau des passeports (un organisme de service spécial relevant du ministère des Affaires étrangères et du Commerce international) recueille les renseignements relatifs aux demandes de passeports en application d'un décret, le *Décret sur les passeports canadiens*, lequel habilite le ministre à prescrire le formulaire à utiliser pour délivrer un passeport. Depuis le 11 septembre 2001, une troisième page a été ajoutée au formulaire de demande en réaction aux préoccupations du Ministère relativement à la sûreté du processus. Sur cette troisième page, le demandeur doit indiquer ses adresses pour une période remontant à deux ans ainsi que fournir des références.

Puisque le passeport constitue une preuve d'identité et de citoyenneté du détenteur lorsque celui-ci se trouve à l'étranger, sa validité dépend fortement de l'exactitude de la déclaration du demandeur. Confirmer les renseignements reçus auprès de répondants qui connaissent le demandeur depuis au moins deux ans permet d'attester de l'exactitude des renseignements. Toutefois, si un demandeur n'est pas en mesure de produire des références, il peut remplir le formulaire *PPT 132-Déclaration fautive de répondant*. Il peut également, dans certaines circonstances, donner le nom d'un membre de sa famille.

Le Bureau des passeports a confirmé qu'il ne pouvait accepter à titre de pièce d'identité supplémentaire un passeport expiré ou un certificat de naissance canadien, car ces

responsable d'assurer la communication légitime de l'information au contrevenant. Les responsables de la CNLC ont de plus maintenu qu'en faisant part au contrevenant de « l'essentiel » du rapport, le SCC aurait respecté toutes les exigences de la loi. Malheureusement, personne au SCC n'avait lu le rapport avant de le remettre au contrevenant ; ces personnes non plus, donc, n'en connaissaient pas le contenu.

De l'avis du CPVP, cette affaire est extrêmement troublante, compte tenu des antécédents du contrevenant, de la nature des renseignements personnels que contenait le rapport, et du fait que le contrevenant résidait chez la plaignante. Le Commissariat a reconnu que la CNLC et le SCC subsistaient des pressions pour placer le contrevenant en résidence le plus rapidement possible et que la communication des renseignements ne dissimulait aucun motif malveillant. Néanmoins, nous avons été consternés d'apprendre que les renseignements personnels de la femme avaient été communiqués pour la simple raison que personne n'avait pris le temps de lire le rapport. Ces renseignements personnels n'auraient jamais dû être communiqués. La *Loi sur la protection des renseignements personnels* est en vigueur depuis 1983 et les fonctionnaires fédéraux se font constamment rappeler leur obligation de protéger les renseignements personnels.

Le Commissariat a conclu que le SCC avait gravement enfreint le droit à la confidentialité de la plaignante ; la plainte était fondée. Malheureusement, la *Loi sur la protection des renseignements personnels* ne prévoit aucun recours ou motifs de révision judiciaire pour les cas de communication inappropriée de renseignements personnels.

Après ce litige, le SCC s'est engagé à ne plus fournir les rapports de placement à la CNLC.

Un passeport expiré est une preuve d'identité insuffisante... pour une demande de passeport

Un homme qui souhaitait renouveler son passeport pour participer à une conférence en Suède s'est demandé :

- pourquoi il fallait fournir des renseignements additionnels aux fins d'identification ;
- pourquoi un passeport expiré ne constituait pas une preuve d'identification suffisante, alors qu'il avait été émis par les autorités fédérales compétentes ; et
- dans quelles circonstances le Bureau des passeports pouvait refuser un document délivré par une autorité fédérale compétente.

deux des références que la femme avait données au SCC. Il a également présenté une copie complète du rapport de placement dans une maison privée – un document que la femme n'avait elle-même jamais vu. Le rapport contenait des renseignements sur les membres de la famille de la femme – dont des renseignements au sujet de mauvais traitements à l'enfance, ses antécédents matrimoniaux et son état civil actuel, et ses antécédents en matière d'études et de travail.

Bouleversée par les révélations du contrevenant, la plaignante a contacté les agents de libération conditionnelle du bureau local du SCC. Ils ont accepté qu'elle sorte le rapport de la chambre du contrevenant et qu'elle masque les noms et numéros de téléphone de ses références dans le carnet d'adresses.

L'enquête a permis de démontrer que les responsables du SCC avaient d'abord eu l'intention de placer le contrevenant dans un autre établissement, mais qu'ils avaient dû modifier leur plan. Ils avaient donc dû obtenir l'autorisation de la CNLC pour changer d'établissement. La situation particulière du contrevenant ainsi que le niveau de soins qu'il nécessitait ont incité les membres de la Commission nationale des libérations conditionnelles à demander des renseignements additionnels au sujet du placement en résidence privée. Le SCC a remis le rapport de placement à la CNLC ; le rapport a été transmis aux membres de la Commission qui ont ensuite approuvé le changement d'établissement. L'enquêteur était convaincu que le contrevenant n'avait communiqué les renseignements à quiconque.

Ce qui était en cause était de savoir si le SCC avait contrevenu à la *Loi sur la protection des renseignements personnels* en remettant son rapport au contrevenant. La *Loi sur le système correctionnel et la mise en liberté sous condition* (LSCMLC) oblige la Commission à faire part au contrevenant des renseignements qui ont permis de prendre une décision à son sujet. Toutefois, il est possible de présenter l'essentiel des renseignements ou encore un résumé de ceux-ci. La LSCMLC autorise aussi la Commission « à refuser la communication de renseignements au délinquant, dans la mesure jugée strictement nécessaire » (paragraphe 144(4)) si la communication peut mettre en danger la sécurité d'une personne ou du pénitencier ou compromettre la tenue d'une enquête en vertu de la loi.

L'enquête a clairement établi que seuls les membres de la Commission nationale des libérations conditionnelles qui devaient prendre une décision en regard à la demande avaient lu le rapport de placement. Personne d'autre à la Commission n'avait lu le rapport intégral, donc personne ne connaissait exactement la quantité et la nature des renseignements personnels qu'il contenait. La CNLC a affirmé que le SCC était

l'étendue du consentement était dictée par le libellé du protocole d'entente (PE) avec le ministère de la Santé. Les mots-clés du formulaire de consentement sont : « pertinents et uniquement aux fins de détermination, de vérification et d'administration du taux de mes prestations... » [traduction].

Afin de déterminer exactement quels renseignements répondent à ces critères, l'enquêteur a la protection de la vie privée examinée le PE et a confirmé que l'ADRC fournissait au régime d'assurance-médicaments uniquement trois montants relatifs au revenu : les lignes 236 – revenu net, 303 – montant pour conjoint, et 5105 – revenu net du conjoint tel qu'il est indiqué pour le calcul du crédit pour la TPS.

Le plaignant s'est montré satisfait des conclusions de l'enquêteur et a apprécié les efforts déployés par le Commissariat pour déterminer le fonctionnement du régime. Il ne souhaitait pas poursuivre de démarches additionnelles et la plainte a été considérée réglée en cours d'enquête.

Communication des renseignements personnels d'une soignante à un contrevenant

Une femme s'est plainte que le Service correctionnel du Canada (SCC) ait fourni une quantité considérable de renseignements personnels la concernant à un contrevenant dont elle prenait soin.

Cette femme fournit à son domicile des soins palliatifs aux personnes âgées et aux gens ayant des besoins particuliers. Le SCC a procédé à une évaluation de la plaignante afin de déterminer si sa résidence constituait un établissement adéquat où placer des contrevenants ayant des besoins particuliers. Des agents du SCC ont visité son domicile, effectué une entrevue détaillée, rédigé un rapport de placement dans une maison privée et ont ensuite approuvé l'usage des services de l'établissement. Par la suite, la femme a accepté d'accueillir un contrevenant à qui la Commission nationale des libérations conditionnelles (CNLC) venait d'accorder une semi-liberté. Le contrevenant devait être placé dans un établissement possédant les ressources pour traiter ses troubles physiques et mentaux tout en respectant les modalités de la libération conditionnelle. Le SCC estime que le contrevenant est un agresseur d'enfants impénitent et qu'il risque de récidiver.

Après approbation, le contrevenant a été confié aux soins de la femme et il a écrit à cette dernière pour lui dire qu'il avait vu son rapport de la CNLC et qu'il était conscient de ses problèmes. Le jour suivant son arrivée au domicile de la plaignante, il a sorti son carnet d'adresses dans lequel il avait inscrit le nom et les numéros de téléphone de

Le personnel de la GRC a obtenu une partie des renseignements, mais le psychologue a refusé de fournir les données psychométriques et ce qu'il qualifiait de « notes personnelles », à moins qu'il ne reçoive une ordonnance d'un tribunal. Il a fait valoir que la communication de ces documents constituerait une transgression des normes de sa profession en matière d'éthique.

Les tentatives de persuasion de la GRC ont été vaines jusqu'à ce que le CPVP, dans une lettre officielle au commissaire de la GRC, avise ce dernier que puisque la GRC avait fait appel aux services du psychologue pour évaluer un de ses membres, tous les renseignements établis ou engendrés à la suite de cette évaluation demeuraient « sous l'autorité » de la GRC en vue de l'application de la *Loi sur la protection des renseignements personnels*. Le psychologue a finalement fourni ses notes ainsi que les données psychométriques à la GRC qui les a fait parvenir au médecin de la plaignante aux fins d'explication et d'interprétation.

Le Commissariat a conclu que la plaignante avait finalement reçu les renseignements adéquats, mais que sa plainte était fondée. Nous avons rappelé à la GRC que les renseignements personnels recueillis par des experts indépendants au nom de la GRC demeuraient sous l'autorité de cette dernière et que les personnes pouvaient donc y avoir accès. Les contrats devraient donner cette information.

La communication de renseignements relatifs à l'impôt sur le revenu est plus limitée qu'il n'était cru au départ

Un homme s'est plaint que son régime provincial d'assurance-médicaments exige qu'il fournisse des renseignements concernant son impôt sur le revenu pour y avoir droit.

Le régime provincial d'assurance-médicaments fournit une aide financière aux personnes pour le paiement de leurs médicaments sur ordonnance. La contribution du régime dépend du revenu familial net – plus celui-ci est bas, plus la contribution du régime est élevée. Il n'est donc pas surprenant d'apprendre que, pour vérifier le revenu du demandeur, le régime demande à ce dernier qu'il consente à ce que l'Agence du revenu du Canada (ARC) lui communique l'information relative à son revenu.

Toutefois, le formulaire de consentement est très général et semble permettre aux responsables du régime de consulter la presque totalité de la déclaration de revenus d'une personne. L'enquêteur à la protection de la vie privée a effectué un suivi auprès de la Division des affaires fédérales-provinciales de l'ARC. Le personnel a expliqué que

Suivi effectué après les enquêtes

Après qu'une enquête a été menée au sujet d'une plainte et que celle-ci est terminée, tout n'est pas clos. Toutes les plaintes se rapportant à la collecte, à l'utilisation, à la communication ou à la conservation inappropriée qui sont considérées fondées sont envoyées à la Direction de la vérification et de la revue aux fins d'examen. Cela permet à la Direction de déterminer des tendances en matière de violation de la protection de la vie privée et d'utiliser cette information pour la planification et l'élaboration des vérifications de l'année suivante.

Cas choisis en vertu de la Loi sur la protection des renseignements personnels

Les cas présentés ci-dessous ont été choisis pour leur valeur éducative. Ils démontrent l'importance du traitement adéquat de renseignements personnels et des problèmes qui peuvent se présenter s'ils ne sont pas traités adéquatement. Nous espérons qu'ils encourageront les institutions et les organismes gouvernementaux à faire preuve d'une vigilance soutenue afin que ceux-ci traitent les renseignements personnels en conformité avec la Loi et s'emploient à donner une formation continue à leur personnel en cette matière. En plus, le grand public pourrait être amené à poser des questions sur la façon dont les institutions fédérales traitent ses renseignements personnels et doit savoir qu'il peut porter plainte auprès du Commissariat lorsque quelque chose ne va pas.

Les notes d'un psychologue indépendant demeurent « sous l'autorité » de la GRC

Une employée de la GRC, sous enquête suite à des allégations de menaces et de recours illégal à une arme à feu, s'est plainte que le corps policier lui ait refusé l'accès aux renseignements recueillis au cours de l'enquête. La plaignante n'avait reçu ni la copie d'une entrevue vidéo ni les notes et données psychométriques résultant de ses entretiens avec un psychologue.

L'enquêteur à la protection de la vie privée a déterminé qu'en plus de certains renseignements dont elle avait fait la requête, l'entrevue vidéo menée par un enquêteur de la GRC renfermait des renseignements sur d'autres personnes, ce qui constituait une exemption prévue par la *Loi sur la protection des renseignements personnels*. La GRC a réussi à supprimer ces segments afin de lui fournir les renseignements restants.

Toutefois, la question des dossiers du psychologue demeurerait problématique. La GRC ne possédait pas de copies de ces documents puisque les services n'avaient pas été fournis par un membre du personnel, mais par un professionnel indépendant, selon le principe de la rémunération des services. Devant l'insistance de l'enquêteur,

TEMPS DE TRAITEMENT DES ENQUÊTES SUR LES PLAINTES – LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le tableau suivant représente le nombre de mois moyen pris pour le règlement d'une enquête sur une plainte selon la conclusion, à partir de la date de réception de la plainte à la date de la conclusion.

Par conclusion

Du 1^{er} avril 2004 au 31 mars 2005

Conclusion	
Réglée rapidement	2,2
Fondée	6,1
Non fondée	6,1
Abandonnée	6,7
Réglée en cours d'enquête	10,1
Fondée et résolue	11,5
Résolue	12,0
Moyenne générale	6,4

Type de plainte	
Correction/Annotation – délais	4,1
Avis de prorogation	4,4
Délais	5,6
Accès	6,3
Utilisation et communication	7,2
Collecte	9,4
Conservation et retrait	10,0
Correction/Annotation	10,7
Moyenne générale	6,4

Le tableau suivant représente le nombre moyen de mois pris pour terminer une enquête sur une plainte selon le type de plainte, à partir de la date de réception de la plainte au moment de la conclusion.

Par type de plainte

Du 1^{er} avril 2004 au 31 mars 2005

À l'examen de ce tableau, on constate que les enquêtes sur les plaintes les moins complexes (délais et avis de prorogation) ont été terminées en moins de temps que les cas les plus complexes. Il s'agit d'une situation normale, car les plaintes plus complexes nécessitent plus d'entrevues sur les lieux, plus de recherche et d'analyse en profondeur et, souvent, de plus longues négociations avec l'institution au sujet des mesures correctrices proposées quand il y a eu une violation de la Loi.

Analyse :

L'enquêteur analyse les faits et prépare les recommandations pour la commissaire à la protection de la vie privée ou son délégué. L'enquêteur communiquera avec les parties et revot les faits recueillis au cours de l'enquête. Il informe également les parties de ce qu'il recommande à la commissaire à la protection de la vie privée ou à son délégué, selon les faits. À cette étape, les parties peuvent fournir d'autres observations. L'analyse comprendra des consultations internes avec, par exemple, les Services juridiques ou la Direction de recherche et politique, au besoin.

Conclusion :

La commissaire à la protection de la vie privée ou son délégué revoit le dossier et évalue le rapport. C'est la commissaire à la protection de la vie privée ou son délégué, et non l'enquêteur, qui décide de l'issue appropriée du dossier et qui décide s'il est approprié de formuler des recommandations pour l'institution.

La commissaire à la protection de la vie privée ou son délégué envoie les lettres expliquant ses conclusions aux parties. Les lettres soulignent le fondement de la plainte, les constatations pertinentes des faits, l'analyse et toute recommandation faite à l'institution. La commissaire à la protection de la vie privée ou son délégué peut demander à l'institution de répondre par écrit, dans un délai précis, pour expliquer les plans prévus pour mettre en œuvre les recommandations.

Les conclusions possibles sont les suivantes :

Non fondée : La preuve ne permet pas à la commissaire à la protection de la vie privée ou à son délégué de conclure que les droits du plaignant en vertu de la Loi ont été enfreints.

Fondée : L'institution a failli à ses obligations face à une disposition de la Loi.

Fondée et résolue : L'enquête a permis d'éteindre les allégations et l'institution a convenu de prendre les mesures correctives pour rectifier le problème.

Fondée : L'institution a failli à ses obligations face à une disposition de la Loi.

Fondée et résolue : L'enquête a permis d'étoffer les allégations et l'institution a convenu de prendre les mesures correctrices pour rectifier le problème.

Résolue : La preuve recueillie au cours de l'enquête soutient les allégations soulevées dans la plainte mais l'institution a convenu de prendre des mesures correctrices pour rectifier le problème à la satisfaction du Commissariat. Cette décision est prise dans le cas de plaintes où il serait trop sévère de dire que la plainte était fondée, étant donné qu'il s'agissait essentiellement d'un problème de communication.

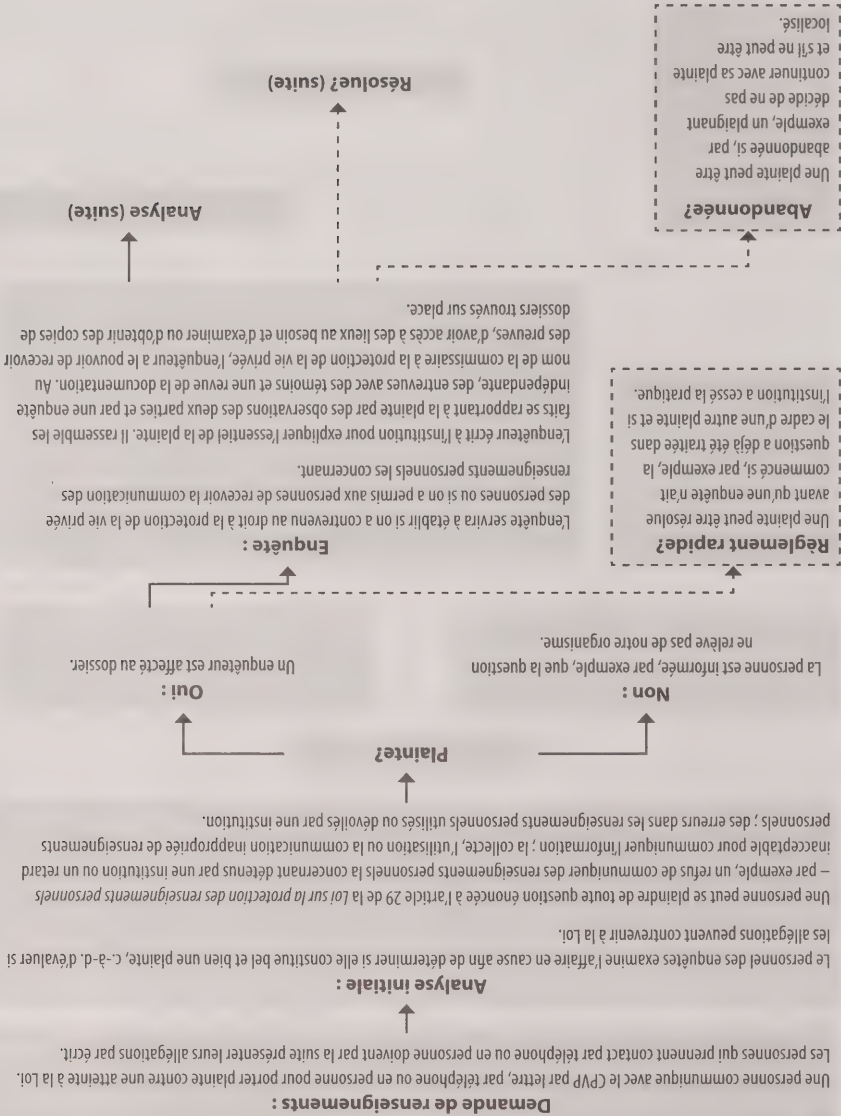
Dans la lettre de conclusions, la commissaire a la protection de la vie privée ou son délégué informe le plaignant de ses droits de recours à la Cour fédérale au sujet du refus de communication de renseignements personnels.

Quand des recommandations sont faites à l'institution, le personnel du CPVP effectuera un suivi pour vérifier si elles ont bel et bien été appliquées.

Le plaignant ou la commissaire a la protection de la vie privée peut choisir de s'adresser à la Cour fédérale pour un refus de communication de renseignements personnels. La Cour fédérale a le pouvoir de revoir l'affaire et de déterminer si l'institution doit fournir l'information au requérant.

Note : une ligne brisée (---) indique un résultat possible.

Processus d'enquête en vertu de la loi sur la protection des renseignements personnels



PLAINTES TERMINÉES ET RÉSULTATS PAR RÉPONDANT (suite)

Plaintes conclues entre le 1^{er} avril 2004 et le 31 mars 2005

Ce tableau indique le nombre de plaintes conclues par répondant et par conclusion.

Répondant	Abandonnée	Réglée	Non fondée	Résolue	Réglée en cours d'enquête	Fondée	Fondée et résolue
Commission nationale des libérations conditionnelles	1	0	15	0	1	1	18
Condition féminine Canada	0	0	2	0	0	0	2
Conseil national de recherches du Canada	0	0	0	0	1	0	1
Défense nationale	5	4	10	4	15	33	71
Développement social Canada	0	0	1	0	3	2	6
Diversification de l'économie de l'Ouest Canada	3	0	0	0	0	0	3
Enquêteur correctionnel du Canada	0	0	2	0	0	1	4
EDULINX Canada Corporation	0	1	0	0	0	0	1
Environnement Canada	0	0	1	0	0	0	1
Finances Canada	0	0	0	0	0	0	1
Gendarmerie royale du Canada	15	5	33	1	19	43	117
Industrie Canada	0	0	1	1	1	0	3
Justice Canada	1	2	3	1	3	7	17
Monnaie royale canadienne	0	0	1	0	0	0	1
Musée canadien des civilisations	0	1	0	0	0	0	1
Musée des beaux-arts du Canada	0	0	0	0	1	0	1
Patrimoine canadien	0	0	1	0	0	0	1
Pêches et Océans	0	0	4	0	0	0	5
Ressources humaines et Développement des compétences Canada	12	9	26	1	8	6	65
Santé Canada	1	0	2	1	2	6	13
Service canadien du renseignement de sécurité	1	0	16	0	9	1	27
Service correctionnel Canada	12	20	1 112 *	5	54	305	1 510
Société canadienne des postes	5	9	29	0	12	37	95
Société canadienne d'hypothèques et de logement	0	0	0	0	0	0	1
Solliciteur général du Canada	0	0	0	0	0	2	2
Statistique Canada	1	1	2	0	0	0	4
Transports Canada	0	1	4	1	2	2	11
Travaux publics et Services gouvernementaux Canada	0	0	2	0	4	0	7
Total	95	87	1 413	22	205	562	2 407

* Le tableau indique clairement que le SCC a traité de façon appropriée un grand nombre de demandes d'accès à l'information en provenance des agents de correction, et ce, conformément aux exigences de la Loi.

PLAINTES TERMINÉES ET RÉSULTATS PAR RÉPONDANT

Plaintes conclues entre le 1^{er} avril 2004 et le 31 mars 2005

Ce tableau indique le nombre de plaintes conclues par répondant et par conclusion.

Répondant	Abandonnée	Réglée rapidement	Non fondée	Réglée	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
Affaires étrangères et Commerce international Canada	0	1	5	0	3	9	0	18
Affaires indiennes et du Nord Canada	0	1	0	0	5	0	0	6
Agence canadienne d'inspection des aliments	0	1	0	0	1	1	0	3
Agence des douanes et du revenu du Canada	28	2	56	3	28	16	3	136
Agence des services frontaliers du Canada	0	7	0	0	0	2	0	9
Agence du revenu du Canada	2	11	41	3	2	26	0	85
Agence spatiale canadienne	0	0	1	0	0	0	0	1
Agriculture et Agroalimentaire Canada	0	0	2	0	1	0	0	3
Anciens Combattants Canada	1	1	3	0	0	0	0	5
Archives nationales du Canada	0	0	2	0	0	0	0	2
Banque de développement du Canada	0	0	0	0	1	0	0	1
Bureau de l'Ombudsman de la Défense nationale et des Forces canadiennes	0	0	0	0	0	0	1	1
Bureau du Conseil privé	0	0	0	0	0	1	0	1
Bureau du vérificateur général du Canada	0	0	1	0	0	0	0	1
Centre d'analyse des opérations et déclarations financières du Canada	0	0	1	0	0	1	0	2
Centre des armes à feu Canada	1	1	0	0	0	0	0	2
Citoyenneté et Immigration Canada	6	7	26	0	22	52	2	115
Commission canadienne des droits de la personne	0	0	0	1	0	1	0	2
Commission canadienne du tourisme	0	0	0	0	0	3	1	4
Commission d'appel des pensions	0	0	0	0	1	0	0	1
Commission des plaintes du public contre la GRC	0	0	1	0	0	2	0	3
Commission de l'immigration et du statut de réfugié	0	0	4	0	6	2	0	12
Commission de la capitale nationale	0	1	0	0	0	0	0	1
Commission de la fonction publique du Canada	0	1	3	0	0	0	0	4

PLAINTES TERMINÉES SELON LA PROVENANCE

Plaintes conclues entre le 1^{er} avril 2004 et le 31 mars 2005

Ce tableau présente la province d'où provenaient les plaintes pour lesquelles des enquêtes ont été menées au cours de l'exercice visé par ce rapport. Notez que certaines plaintes nous sont parvenues de personnes habitant à l'extérieur du Canada.

Province/Territoire	Total
Québec	1 090*
Ontario	641*
Colombie-Britannique	274
RCN (ON)	106
Alberta	81
Nouveau-Brunswick	59
Saskatchewan	40
RCN (QC)	39
Manitoba	34
Nouvelle-Écosse	17
Ile-du-Prince-Édouard	6
Extérieur du Canada	6
Terre-Neuve et Labrador	5
Territoires du Nord-Ouest	3
Nunavut	3
Territoire du Yukon	3
Total	2 407

* Un nombre considérable de plaintes parmi celles illustrées par ces chiffres sont attribuables aux plaintes déposées par les agents de correction du SCC.

Pour les plaintes conclues entre le 1^{er} avril 2004 et le 31 mars 2005

selon le type de plainte pour l'année visée par ce rapport.

	Abandonnée	Réglée	Non fondée	Réglée	Réglée	Fondée	Fondée	Total	Pourcentage
Accès	44	22	1 170*	18	120	21	21	1 416	59 %
Correction/Annotation	1	0	5	0	3	0	0	9	0 %
Langue	1	0	0	1	0	0	0	2	0 %
Collecte	3	11	32	2	12	6	0	66	3 %
Conservation et retrait	0	2	7	0	2	2	1	14	1 %
Utilisation et communication	29	43	143	1	63	138	1	418	17 %
Délais	15	9	42	0	5	361**	0	432	18 %
Avis de prorogation	1	0	14	0	0	23	0	38	2 %
Correction/Délais	1	0	0	0	0	11	0	12	0 %
Total (# et %)	95 (4 %)	87 (4 %)	1 413 (59 %)	22 (1 %)	205 (8 %)	562 (23 %)	23 (1 %)	2 407	100 %

* Comme il a été mentionné précédemment, une grande partie des plaintes jugées non fondées ont été déposées par des agents de correction du SCC, qui ont invoqué les dispositions de la Loi en matière d'accès à l'information et ses mécanismes subsidiaires de traitement des plaintes, dans le cadre de leur conflit de travail en cours avec le SCC. Dans ces cas, le SCC a décidé de fournir aux agents de correction les renseignements personnels qui les concernent en utilisant une méthode particulière d'accès à l'information à laquelle les agents de correction se sont opposés. L'enquête ultérieure du Commissariat concernant ces plaintes a établi que le SCC pouvait choisir sa méthode d'accès à l'information et, ce faisant, qu'il respectait la Loi sur la protection des renseignements personnels.

Un grand nombre de plaintes concernant les délais ont été déposées contre certains ministères faisant face à de sérieux problèmes de ressources. Même si le Commissariat peut comprendre les préoccupations des ministères, la Loi sur la protection des renseignements personnels ne fournit aucune possibilité de refuser l'étude de ces plaintes. Les ministères et les organismes sont tenus de répondre à toutes les demandes de communication de renseignements personnels, et le rôle du Commissariat est de veiller à ce que les ministères appliquent correctement la Loi sur la protection des renseignements personnels. Cela dit, le Commissariat est conscient que certains institutions abordent présentement la question du ressourcement et il les félicite de leur démarche à cet égard. Nous attendons avec intérêt de voir les répercussions qu'auront les nouvelles ressources sur le nombre de plaintes et nous en ferons part dans notre prochain rapport annuel.

Réglée : après une enquête approfondie, le Commissariat a participé à la négociation d'une solution satisfaisant les deux parties. Cette conclusion est réservée aux plaintes pour lesquelles une conclusion *fondée* serait trop sévère compte tenu que la situation relève essentiellement d'une mauvaise communication ou d'un malentendu.

Résolue en cours d'enquête : le Commissariat a participé à la négociation d'une solution satisfaisant toutes les parties dans le cadre de l'enquête. Aucune conclusion n'est rendue.

Abandonnée : l'enquête a pris fin avant que toutes les allégations soient pleinement examinées. Une affaire peut être *abandonnée* pour toutes sortes de raisons ; par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, lesquels sont essentiels pour arriver à une conclusion.

Réglée rapidement : le Commissariat a commencé à utiliser cette nouvelle disposition en avril 2004 pour traiter des situations où l'affaire est réglée avant même qu'une enquête officielle ne soit entamée. À titre d'exemple, si une personne dépose une plainte dont le sujet a déjà fait l'objet d'une enquête par le Commissariat et a été considéré conforme à la *Loi sur la protection des renseignements personnels*, nous lui expliquons la situation. Nous avons en outre reçu des plaintes pour lesquelles une enquête officielle aurait pu avoir des retombées négatives sur la personne. En pareil cas, nous expliquons en profondeur la situation au plaignant. Si la personne décide alors de ne pas poursuivre l'affaire, celle-ci est « *réglée rapidement* ».

Même s'il a conclu plus de plaintes relatives à la *Loi sur la protection des renseignements personnels* qu'il n'en a reçues, le Commissariat procède, en fin d'exercice financier, au suivi d'un nombre considérable de cas, soit 1 277. Les ressources ont été insuffisantes pour répondre à la demande. En fin d'exercice se sont déroulées les dernières étapes d'un examen approfondi des processus opérationnels de la Direction, dont le but était de simplifier les processus, dans la mesure du possible, de collaborer à l'évaluation des niveaux de ressources appropriés et de traiter le problème lié au nombre croissant de cas en cours de traitement.

En temps normal, le Commissariat termine environ 1 185 plaintes avec le personnel en place. Compte tenu des 1 500 requêtes excédentaires reçues chaque année, nous perdons du terrain; bon nombre de cas en attente se font vieux et à la fin de l'exercice, 577 plaintes n'ont toujours pas été assignées en raison du manque d'effectifs. Nous avons limité la charge de travail d'un enquêteur à un maximum de 35 cas actifs de front. Certains des cas non assignés sont maintenant en attente depuis presque un an. Des plaintes plus anciennes encore, en cours d'enquête, nécessitent plus de temps puisque les délais ont des répercussions néfastes sur l'accessibilité aux documents et sur la mémoire des personnes impliquées. Selon les normes établies par la Direction selon lesquelles les enquêteurs complètent 75 cas par année, il faudrait environ huit enquêteurs au cours d'une année pour s'occuper uniquement des cas non assignés.

Définitions des conclusions en vertu de la *Loi sur la protection des renseignements personnels*

Le Commissariat a élaboré une série de définitions de conclusions qui expliquent les résultats des enquêtes se déroulant en vertu de la *Loi sur la protection des renseignements personnels*.

Non fondée : L'enquête n'a pas permis de déceler des éléments de preuve qui suffisent à conclure que l'Institution fédérale n'a pas respecté les droits d'un plaignant aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée : L'Institution fédérale n'a pas respecté les droits d'une personne aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée et résolue : les allégations sont corroborées par l'enquête et l'Institution fédérale a accepté de prendre des mesures correctives pour remédier à la situation.

PLAINTES REÇUES SELON LE RÉPONDANT (suite)

Plaintes reçues entre le 1^{er} avril 2004 et le 31 mars 2005

Ce tableau présente le nombre total de plaintes déposées contre les différents ministères et organismes reçues au cours de la période visée par ce rapport.

Gendarmerie royale du Canada **	155
Industrie Canada	3
Justice Canada	32
L'Enquêteur correctionnel Canada	2
Musée des beaux-arts du Canada	2
Pêches et Océans	8
Ressources humaines et Développement des compétences Canada	41
Ressources naturelles Canada	8
Santé Canada	27
Service canadien du renseignement de sécurité	49
Service correctionnel du Canada ***	395
Société canadienne des postes	60
Statistique Canada	1
Transports Canada	1
Travaux publics et Services gouvernementaux Canada	3
Total	1 571

** GRC - Un grand nombre de plaintes concerne le temps de traitement, car la GRC n'a pas été en mesure de répondre aux demandes dans les délais prescrits par la Loi.
 *** SCC - Les agents de correction ont déposé une grande partie des plaintes dans le cadre de la négociation de leurs relations de travail avec l'employeur.

Plaintes terminées

Le nombre de plaintes terminées s'élève à 2 407, soit 800 de plus que le nombre de plaintes reçues au Commissariat au cours de l'année. Toutefois, près d'un millier de plaintes provenaient d'un même groupe de personnes : les agents de correction demandaient qu'on leur fournisse leurs dossiers personnels. Comme plusieurs de ces plaintes étaient similaires, elles exigeaient moins de travail que ne l'auraient nécessités 1 000 plaintes distinctes ; à titre d'exemple, les documents afférents à une plainte terminée servaient de modèles pour plusieurs autres plaintes. Néanmoins, les enquêteurs ont accompli un travail remarquable pour conclure un si grand nombre de cas, surtout qu'il y avait moins de personnel qu'au cours des années précédentes, et que les enquêteurs ont été affectés à tour de rôle à l'Unité des demandes de renseignements à court d'effectifs.

PLAINTES REÇUES SELON LE RÉPONDANT

Plaintes reçues entre le 1^{er} avril 2004 et le 31 mars 2005

Ce tableau présente le nombre total de plaintes déposées contre les différents ministères et organismes reçues au cours de la période visée par ce rapport.

Institutions	
Affaires étrangères et Commerce international Canada	24
Affaires indiennes et du Nord Canada	4
Agence canadienne d'inspection des aliments	2
Agence de gestion des ressources humaines de la fonction publique du Canada	1
Agence de promotion économique du Canada atlantique	1
Agence des douanes et du revenu du Canada	6
Agence des services frontaliers du Canada	26
Agence du revenu du Canada	183
Agriculture et Agroalimentaire Canada	2
Anciens Combattants Canada	5
Archives nationales du Canada	3
Banque du Canada	1
Bureau du Conseil privé	1
Bureau du directeur général des élections	11
Centre d'analyse des opérations et déclarations financières du Canada	1
Centre des armes à feu Canada	1
Citoyenneté et Immigration Canada	118
Commission canadienne de sûreté nucléaire	1
Commission canadienne des droits de la personne	3
Commission d'examen des plaintes concernant la police militaire	1
Commission de l'immigration et du statut de réfugié *	222
Commission de la capitale nationale	5
Commission de la fonction publique du Canada	6
Commission des plaintes du public contre la GRC	3
Commission des relations de travail dans la fonction publique	1
Commission nationale des libérations conditionnelles	10
Conseil de recherches en sciences naturelles et en génie	1
Conseil national de recherches du Canada	47
Défense nationale	72
Développement social Canada	18
Diversification de l'économie de l'Ouest Canada	3
École de la fonction publique du Canada	1
Elections Canada	1
Environnement Canada	4
Financement agricole Canada	1

* CISR – Une personne a déposé un nombre important de plaintes dans le cadre de ses échanges avec la CISR.

PLAINTES REÇUES SELON LE TYPE DE PLAINTE

Plaintes reçues entre le 1^{er} avril 2004 et le 31 mars 2005

Ce tableau indique le nombre de plaintes reçues en fonction du type de plainte.

Type de plainte	Total	Pourcentage
Accès	604	38 %
Correction/Annotation	29	2 %
Langue	2	0 %
Collection	92	6 %
Conservation et retrait	17	1 %
Utilisation et communication	250	16 %
Délais	489	31 %
Avis de prorogation	90	6 %
Correction – délais	4	0 %
Total	1 577	100 %

LES DIX PREMIERS MINISTÈRES SELON LE NOMBRE DE PLAINTES REÇUES

Exercice se terminant le 31 mars 2005

Ce tableau présente les ministères ayant reçu le plus grand nombre de plaintes au cours de la période visée par ce rapport.

Veuillez noter que cela ne signifie pas nécessairement que ces ministères ne se conforment pas à la *Loi sur la protection des renseignements personnels*. Certains de ces ministères, en raison de leur mandat, détiennent une grande quantité de renseignements personnels concernant des personnes et reçoivent donc vraisemblablement plus de demandes d'accès à l'information. Un plus grand nombre de renseignements personnels entraîne une augmentation possible du nombre de plaintes sur les activités de ces ministères en matière de collecte, d'utilisation, de communication, de conservation et de retrait des renseignements personnels ainsi que sur sa façon de procurer l'accès à cette information.

Institutions	Total	Accès	Délais	Vie privée
Service correctionnel Canada	395	162	84	149
Commission de l'immigration et du statut de réfugié	222	96	126	0
Agence du revenu du Canada	183	69	64	50
Gendarmerie royale du Canada	155	58	67	30
Citoyenneté et Immigration Canada	118	39	72	7
Défense nationale	72	25	34	13
Société canadienne des postes	60	32	1	27
Service canadien du renseignement de sécurité	49	46	2	1
Conseil national de recherches Canada	47	0	46	1
Justice Canada	32	14	17	1
Autres	244	94	70	80
Total	1 577	635	583	359

- **Frais.** Des frais ont été établis au regard d'une demande de renseignements en vertu de la *Loi sur la protection des renseignements personnels* ; aucuns frais ne sont présentement prévus pour l'obtention de renseignements personnels.
- **Répertoire.** INFOSOURCE¹ ne décrit pas de façon adéquate le fonds de renseignements personnels que détient une institution.

Renseignements personnels :

- **Collecte.** Collecte de renseignements personnels non requis pour l'exploitation d'une activité ou d'un programme de l'institution ; les renseignements personnels ne sont pas recueillis directement auprès de la personne concernée ; la personne n'est pas informée des fins de la collecte des renseignements personnels.

- **Conservation et retrait.** La conservation des renseignements personnels ne respecte pas les calendriers de conservation et de retrait (approuvés par les Archives nationales et publiés dans INFOSOURCE¹) ; ils sont soit détruits trop rapidement, soit conservés trop longtemps.

De plus, les renseignements personnels utilisés à des fins administratives doivent être conservés pendant au moins deux ans après la dernière application d'une mesure administrative, à moins que la personne ne consente à leur retrait.

- **Utilisation et communication.** Les renseignements personnels sont utilisés et communiqués sans le consentement de la personne et ne satisfont pas aux critères de communication permise sans consentement tel qu'il est stipulé au paragraphe 8(2) de la Loi.

Délais :

- **Délais.** L'institution n'a pas répondu à la demande dans les délais prévus par la Loi.
- **Avis de prorogation.** L'institution n'a pas fourni de raison adéquate pour la prorogation, a fait la demande de prorogation après que le délai initial de 30 jours a été dépassé, ou a fixé l'échéance à plus de 60 jours de la date de réception de la demande.

- **Correction/Annotation – délais.** L'institution n'a pas apporté les corrections aux renseignements personnels ou n'a pas annoté les dossiers dans les 30 jours suivant la demande de correction des renseignements.

¹ INFOSOURCE est un répertoire du gouvernement fédéral qui décrit chaque institution et les banques de renseignements (regroupement de dossiers sur un même sujet) qu'elle détient.

Enquêtes et demandes de renseignements

Plaintes reçues

La Loi ne confère pas à la commissaire le pouvoir de rendre des ordonnances. Toutefois, la commissaire peut recommander au besoin des changements relatifs aux pratiques de traitement des renseignements utilisées par les institutions gouvernementales, ce qu'elle fait. Par ailleurs, elle peut mener en tout temps des vérifications auprès de ministères ou d'organismes fédéraux et recommander que soient modifiées les pratiques qui ne sont pas conformes à la *Loi sur la protection des renseignements personnels*.

La commissaire est tenue de déposer un rapport annuel au Parlement sur les activités du Commissariat au cours de l'exercice précédent. Le présent rapport vise la période comprise entre le 1^{er} avril 2004 et le 31 mars 2005 au titre de la *Loi sur la protection des renseignements personnels*.

Av cours de l'exercice 2004-2005, le Commissariat a reçu 1 577 plaintes sous la *Loi sur la protection des renseignements personnels*, en baisse par rapport aux 4 206 plaintes reçues au cours de l'exercice 2003-2004. Bien que cette baisse soit considérable, le nombre de plaintes avait atteint, au cours de l'exercice 2003-2004, un record inégalé en raison de circonstances particulières : près de 500 Autochtones du Canada s'étaient plaints d'un formulaire de consentement de Santé Canada et plus de 2 000 plaintes avaient été déposées à l'endroit de Service correctionnel Canada par des agents de correction, des employés et des détenus. Cette année, le nombre de plaintes est plus près de la normale.

Définition des types de plaintes

Les plaintes que reçoit le Commissariat sont classées selon trois groupes principaux :

Accès :

- **Accès.** Certains renseignements personnels n'ont pas été reçus, soit parce que certains d'entre eux ou certains documents manquent à l'appel, soit parce que l'institution a appliqué des exemptions lui permettant de retenir des renseignements.

- **Correction/Annotation.** L'institution n'a pas apporté les corrections aux renseignements personnels ou n'a pas annoté les dossiers aux endroits où les renseignements ne concordent pas avec les corrections demandées.

- **Langue.** Les renseignements personnels n'ont pas été fournis dans la langue officielle demandée.

La Loi sur la protection des renseignements personnels, en vigueur depuis 1983, protège les renseignements personnels concernant les personnes que détiennent les ministères et les organismes du gouvernement fédéral. La Loi régit la manière dont les institutions fédérales recueillent, utilisent, communiquent, conservent et détruisent des renseignements personnels nécessaires à l'administration des programmes gouvernementaux. Elle confère aux personnes le droit de demander accès à leurs renseignements personnels détenus par le gouvernement et celui de demander que des corrections y soient apportées. De plus, la Loi établit les fonctions, les responsabilités et le mandat de la commissaire à la protection de la vie privée du Canada.

La commissaire reçoit des plaintes de personnes qui estiment que leurs droits en vertu de la Loi sur la protection des renseignements personnels ont été enfreints, et mène des enquêtes. Elle peut également déposer une plainte et mener une enquête de sa propre initiative si elle estime qu'il existe des motifs raisonnables de croire que la Loi a été enfreinte.

La commissaire à la protection de la vie privée du Canada agit à titre d'ombudsman afin de résoudre les plaintes grâce, autant que possible, à la médiation, à la négociation et à la persuasion. Toutefois, la Loi confère à la commissaire de vastes pouvoirs d'enquête lui permettant de s'acquitter de son mandat. Elle peut assigner des témoins à comparaître et à témoigner, pénétrer dans des locaux pour se faire remettre des documents et mener des entrevues. L'entrave aux enquêtes constitue une infraction à la Loi.

recommandons que le SCT développe un cadre-modèle à titre de guide de gestion de la protection de la vie privée pour les ministères et les organismes fédéraux.

Nous avons discuté de nos recommandations au sujet d'un cadre-modèle avec la direction du SCT. Le président du Conseil du Trésor s'est engagé à explorer le concept d'un cadre de gestion de la protection de la vie privée couvrant l'ensemble du gouvernement. Nous sommes au fait que le SCT a commencé un examen de la portée et du processus d'un projet qui s'articulerait à partir de cadres existants. Le projet nécessitera des ressources spécifiques, la coopération des intervenants (dont le Commissariat), la communication active avec les ministères, et des mécanismes de conformité appropriés.

Nous accueillons favorablement cette initiative.

Il incomberait au Conseil du Trésor d'édicter un modèle de cadre de gestion de la protection de la vie privée. Une approche en souplesse serait de mise pour la conception et l'application d'un modèle. Nous recommandons que ce modèle possède les caractéristiques suivantes :

- celles de communiquer efficacement l'importance de la gestion des renseignements personnels et l'engagement à intégrer la protection de la vie privée à la gestion des programmes ;

- celle d'établir des objectifs et des normes clairs sur la collecte, la qualité, l'utilisation, la sécurité, la transmission, l'accès, la communication, la conservation et le retrait des renseignements personnels ;

- celles de clarifier les rôles et les responsabilités et de fournir une base permettant de déterminer les ressources et les compétences nécessaires à l'élaboration d'un cadre solide de gestion de la protection de la vie privée ;

- celles de se fonder sur des approches rigoureuses de gestion des risques, en particulier par l'entremise d'EFVP et d'évaluations de la menace et des risques ;

- celles d'utiliser des contrôles efficaces pour maintenir la conformité et les meilleures pratiques – intégration de la meilleure technologie de confidentialité disponible, résolution de litiges, et détermination et correction des faiblesses du système ou des incidents relatifs à la protection de la vie privée ; et

- celles de promouvoir l'imputabilité et l'amélioration continue par des moyens tels que l'établissement de rapports, la vérification et l'évaluation, la sensibilisation et l'évaluation du rendement.

Puisque le concept est nouveau, il y aura inévitablement des ajustements – amenés par l'expérience et l'expérimentation. En fait, nous procédons à une vérification d'envergure qui nous permettra d'évaluer, de raffiner et de valider notre approche. Une fois cette évaluation complétée, nous prévoyons qu'elle attestera de la valeur d'un cadre de gestion de la protection de la vie privée.

La protection de la vie privée est, à plusieurs égards, une question de gestion des risques. Les cadres de gestion de la protection de la vie privée sont d'une importance capitale pour aider les institutions fédérales à gérer ces risques. Par conséquent, nous

- **gestion du risque** – mise sur pied d'un examen et d'un protocole d'approbation pour l'évaluation des facteurs relatifs à la vie privée, établissement de normes, d'ententes pour l'échange de renseignements personnels et exécution des examens sur les bases de données de recherche ;
- **changement culturel** – formation de tous les gestionnaires, employés et agents contractuels en gestion des renseignements personnels dont une formation spécialisée en fonction des exigences particulières des programmes ; et
- **conformité** – élaboration de normes de vérification interne pour la gestion des renseignements personnels.

RHDDC a constaté que l'adoption d'un cadre de gestion de la protection de la vie privée avait donné au Ministère un nouvel élan pour l'amélioration de la gestion des renseignements personnels. Le cadre a servi de base pour définir de meilleures pratiques en matière de protection de la vie privée et pour l'aider à prendre l'initiative afin de définir et de résoudre les problèmes. Nous saluons le leadership du Ministère et son engagement à favoriser des pratiques équitables en matière de renseignements personnels.

Le soutien des évaluations des facteurs relatifs à la vie privée

L'exécution d'évaluations des facteurs relatifs à la vie privée (EFVP) constitue une autre incitation à l'élaboration d'un cadre solide de gestion de la protection de la vie privée. Depuis mai 2002, la politique du Conseil du Trésor oblige les ministères et les organismes fédéraux à mener des évaluations des facteurs relatifs à la vie privée pour tous les nouveaux programmes ou services présentant des risques potentiels pour la protection de la vie privée. Les évaluations visent à prévoir des problèmes éventuels en matière de protection de la vie privée et à cerner des options qui permettront de diminuer les risques avant la mise en œuvre des projets.

La politique d'EFVP est non seulement un élément clé de toute stratégie judicieuse de gestion de la protection de la vie privée ; elle encourage l'adoption d'une structure qui est essentiellement un cadre de gestion de la protection de la vie privée. Par exemple, les lignes directrices de la politique d'EFVP exigent que les chefs de service précisent les rôles du personnel en ce qui a trait à son adhésion aux exigences de la politique. Les chefs de service doivent aussi assumer la responsabilité de surveiller la mise en application des exigences – responsabilités qui sont au cœur même du cadre de gestion de la protection de la vie privée. La politique sert à la fois d'outil de promotion de la sensibilisation à l'endroit de pratiques solides en matière de protection de la vie privée et à mesurer la conformité d'un ministère aux meilleures pratiques en matière de protection de la vie privée.

Bien que chacune de ces initiatives soit considérable, ensemble, elles expriment la nécessité d'une approche davantage détaillée et cohérente de la gestion de la protection de la vie privée au gouvernement fédéral. Un cadre de gestion de la protection de la vie privée permettrait d'atteindre cet objectif.

En quoi un cadre de gestion de la protection de la vie privée est-il efficace?

Premièrement, ce sont le SCT et les ministères – et non le Commissariat – qui ont la responsabilité d'assurer la mise en place d'un cadre de gestion adéquat de la protection de la vie privée. La conception et la mise en œuvre de cadres doivent être initiées à l'interne plutôt qu'imposées de l'extérieur. Un organisme de surveillance externe tel que le Commissariat peut, et devrait, suggérer les principaux éléments d'un cadre efficace. Nous pouvons également effectuer des examens et des vérifications *a posteriori* afin de déterminer si le cadre fonctionne comme prévu. Toutefois, pour en assurer le succès, la responsabilité du processus revient au ministère.

Le concept de cadre de gestion de la protection de la vie privée semble gagner de la popularité au sein du gouvernement fédéral. Le Comité des Sous-ministres adjoints (SMA) sur la protection de la vie privée (présidé par le SCT, le ministre de la Justice du Canada et le Bureau du Conseil privé) a tenu des rencontres périodiques pour promouvoir une approche fédérale cohérente et efficace à la protection de la vie privée, laquelle comprend l'élaboration d'un cadre général de protection de la vie privée et le partage des meilleures pratiques.

Certains ministères s'attellent déjà au travail. Par exemple, le ministère des Ressources humaines et Développement des compétences Canada (RHDDC) a présenté son cadre de gestion de la protection de la vie privée au Comité des SMA sur la protection de la vie privée en juin 2004. Le Ministère fait un grand usage de données personnelles puisqu'il administre, entre autres, l'assurance-emploi et le Programme canadien de prêts aux étudiants. Le cadre vise à favoriser la confiance des citoyennes et des citoyens en leur fournissant plus d'information sur les programmes du Ministère et sa façon d'utiliser et de communiquer les renseignements personnels.

RHDDC définit ainsi les quatre piliers de son cadre de gestion de la protection de la vie privée :

- **planification stratégique et gouvernance** – recherche et analyse visant à mieux comprendre les attentes des citoyens et des citoyens en matière de protection de la vie privée ; définition des principes de protection de la vie privée au cœur de leurs opérations ;

- des améliorations peuvent être obtenues au moyen de politiques et de lignes directrices ; et
- le Secrétaire du Conseil du Trésor (SCT), comme lieu des politiques en matière de protection de la vie privée, devrait s'assurer que les ministères et les organismes fédéraux rencontrent des normes élevées en matière de gestion de la protection de la vie privée.

Par exemple, en août 2004, le Commissariat a présenté un mémoire au gouvernement sur les répercussions de la *USA PATRIOT Act*. Nous y suggérons que le gouvernement fédéral examine les circonstances dans lesquelles il permettrait que les renseignements personnels des Canadiennes et des Canadiens soient traités à l'extérieur du Canada, donc hors de la protection de la *Loi sur la protection des renseignements personnels*.

La commissaire à la protection de la vie privée a, par la suite, écrit au président du Conseil du Trésor pour lui demander son soutien en cette matière.

En réponse à la lettre de la commissaire, le SCT a entrepris un examen des arrangements pris par le gouvernement fédéral en matière d'impartition des renseignements personnels. Il a aussi commencé à élaborer des modèles de clauses contractuelles à l'usage des ministères afin de réduire les risques potentiels à la protection de la vie privée relatifs aux renseignements personnels traités par des entreprises américaines ou par des sociétés affiliées basées aux États-Unis et assujetties à la *USA PATRIOT Act*. Cette initiative est extrêmement importante, et le SCT s'attend à ce que le travail soit terminé sous peu.

Le Commissariat a également suggéré que le SCT examine les pratiques de couplage et d'assemblage de données qu'effectue le gouvernement fédéral, réexamine la politique surannée sur le couplage de données (1989) et renforce les exigences relatives à l'établissement de rapports au titre de la *Loi sur la protection des renseignements personnels*. Toutes ces activités sont en cours et nous les accueillons favorablement. Nous sommes également satisfaits des exigences relatives à l'établissement de rapports formulées par le SCT en avril 2005.

Les lignes directrices sur l'établissement de rapports suggèrent une volonté à l'égard d'une gestion renforcée de la protection de la vie privée. Lorsque ces lignes directrices auront été mises à l'épreuve, le Commissariat prévoit examiner en profondeur l'établissement de rapports sur la protection de la vie privée afin de déterminer quels rapports annuels et données statistiques expliquent le plus clairement les activités et les enjeux sur la protection de la vie privée, et soutiennent une gestion solide de celle-ci.

Cadre de gestion de la protection de la vie privée

Elaborer un cadre de gestion de la protection de la vie privée à l'intention du gouvernement fédéral

Qu'est-ce qu'un cadre?

En règle générale, les cadres de travail servent de plan pour aider les institutions fédérales à atteindre les résultats souhaités. Ils établissent des objectifs et des politiques ; ils décrivent les systèmes, les procédures et les mesures de rendement nécessaires pour atteindre ces objectifs. S'ils sont bien conçus et mis en application, les cadres peuvent être des instruments puissants en vue de montrer aux institutions la meilleure façon de mener une activité et la façon d'organiser et d'allouer les ressources pour obtenir des résultats.

Bien que le concept ne soit pas nouveau dans les milieux de la gestion, il est lorsqu'il s'agit de l'appliquer sur le plan de la protection de la vie privée. Il faudrait concevoir un modèle de cadre de gestion de la protection de la vie privée à l'échelle gouvernementale pour aider les ministères à protéger les renseignements personnels qu'ils contrôlent en identifiant les risques inhérents à la protection de la vie privée et en identifiant les façons de minimiser ces risques.

L'intérêt du CPVP pour les cadres de gestion de la protection de la vie privée

Le Commissariat cherche constamment à améliorer la manière de gérer la protection de la vie privée au gouvernement. Nous le faisons en présument que :

- la Loi sur la protection des renseignements personnels (en dépit d'une réforme nécessaire) ne devrait pas empêcher la gestion améliorée de la protection de la vie privée ;

Les personnes, ou la commissaire agissant en leur nom, devraient être en mesure de demander à la Cour d'examiner les activités du gouvernement en matière de collecte, d'utilisation et de communication de renseignements personnels. De même la commissaire, à titre de plaignante, devrait pouvoir s'adresser à la Cour pour l'examen de toute affaire qui entre dans le champ d'application de la *Loi sur la protection des renseignements personnels*. Et la Cour devrait être habilitée à fixer des dommages-intérêts pour les institutions prises en défaut.

Si le modèle de l'ombudsman a fait preuve d'efficacité pour éviter les situations de confrontation afin d'encourager l'application de la loi, le fait de faire appel à l'équité et au bon sens n'est efficace que dans la mesure où cela engendre la conformité.

Des modèles dans plusieurs juridictions au Canada et à l'étranger accordent à la personne en charge les outils pour lui permettre de contraindre au respect de la loi. Le Parlement voudra peut-être examiner les avantages à accorder de tels pouvoirs à la commissaire à la protection de la vie privée du Canada.

Activités de recherche et de sensibilisation du grand public

Pendant plusieurs années, les commissaires à la protection de la vie privée qui se sont succédé ont fait valoir que les menaces naissantes à l'endroit de la protection de la vie privée des Canadiennes et des Canadiens justifiaient un discours éclairé et efficace pour la défense de la protection de la vie privée. Le Commissariat a besoin de pouvoirs et de ressources pour mener des activités de recherche et élaborer des rapports sur les enjeux relatifs à la protection de la vie privée, sensibiliser le grand public à son droit à la vie privée, et évaluer l'incidence sur la protection de la vie privée des projets de loi.

Bien que le Parlement ait entendu ces arguments au cours de la rédaction de la *LPRPDE* – et à quel point les outils se sont avérés utiles –, la commissaire ne s'est pas vu octroyer le même mandat de sensibilisation du grand public sous le régime de la *Loi sur la protection des renseignements personnels*. La commissaire devrait déténir les mêmes pouvoirs de sensibilisation des entreprises, du gouvernement et du public en vertu des deux lois.

Renforcer les révisions judiciaires

Finalement, les plaignants – et la commissaire à la protection de la vie privée – peuvent uniquement obtenir un examen judiciaire et un droit de recours suite à un refus d'accès à leurs renseignements personnels. Dans les faits, cela signifie que des allégations de collecte, d'utilisation ou de communication inappropriées ne peuvent être contestées en Cour. Cela signifie également que les avantages qui seraient associées à l'émission de directives de la Cour à l'endroit des institutions gouvernementales sont perdus. La *Loi sur la protection des renseignements personnels* ne prévoit pas non plus de recours pour des préjudices causés par les interventions du gouvernement.

Même après que la commissaire a reconnu que la plainte était justifiée, la Cour fédérale a décidé, en mars 2005 (*Murdoch c. Canada (Gendarmerie royale du Canada)*) que ni la Cour, ni la commissaire à la protection de la vie privée n'avaient de pouvoirs autres que ceux prévus par la *Loi sur la protection des renseignements personnels*.

l'alinéa 8(2)b) de la Loi n'impose pas une telle restriction. L'année suivante, la Cour suprême a déclaré être essentiellement d'accord avec ce jugement.

La Loi sur la protection des renseignements personnels énonce également au paragraphe 8(2) les circonstances spécifiques selon lesquelles les institutions gouvernementales peuvent communiquer des renseignements personnels sans le consentement de la personne. Notamment la communication à des organismes d'enquête désignés, aux Archives publiques, aux députés en vue d'aider des électeurs, à des gouvernements provinciaux ou étrangers, et à des fins de recherche et de statistiques.

Certaines circonstances paraissent trop permissives. Par exemple, l'alinéa 8(2)f) autorise des communications en vertu d'une entente ou d'un arrangement entre le gouvernement du Canada et le gouvernement d'une province ou d'un pays étranger. Cette disposition se doit d'être beaucoup plus précise en ce qui a trait aux paramètres définissant une telle communication, et donner des conseils sur les types de dispositions contractuelles nécessaires pour protéger les renseignements personnels.

Lorsque les Canadiennes et les Canadiens communiquent des renseignements au gouvernement canadien ou à un consulat à l'étranger, ils s'attendent à ce que ces renseignements ne soient pas indûment remis entre les mains d'un État étranger. Le libellé actuel de l'alinéa 8(2)f) est de portée générale et son interprétation est laissée à la discrétion des ministères. Il devrait exiger un examen complet des raisons pour lesquelles l'État étranger requiert ces renseignements, de l'utilisation qui en sera faite, de l'autorité qui en fait la demande, des mesures en place et de leur efficacité pour protéger les renseignements, y compris des dispositions interdisant la communication à des tiers. En attendant la réforme de la Loi sur la protection des renseignements personnels, la commissaire à la protection de la vie privée encourage fortement les institutions gouvernementales à ce qu'elles s'imposent des normes plus sévères.

Après plus de 20 ans à surveiller l'administration de la Loi sur la protection des renseignements personnels, il s'avère évident que les dispositions en matière de communication nécessitent un examen et une révision en profondeur.

Habiller la commissaire à la protection de la vie privée

S'éloigner du rôle de simple « ombudsman »

La Loi sur la protection des renseignements personnels confère à la commissaire à la protection de la vie privée du Canada les pouvoirs d'un ombudsman, sans pouvoirs inhérents à l'application de la loi. Toutefois, la commissaire à la protection de la vie privée peut, dans certaines circonstances, demander l'aide de la Cour fédérale.

- (c) les conséquences dans l'éventualité où les renseignements ne sont pas fournis ; et
- (f) le droit de la personne de porter plainte en vertu de la *Loi sur la protection des renseignements personnels*.

« Accessible au public »

Une exception aux dispositions de la *Loi sur la protection des renseignements personnels* en matière d'utilisation et de communication touche les renseignements « accessibles au public », par exemple les renseignements disponibles dans les archives publiques, les bibliothèques et les musées. Toutefois, ces renseignements comprennent également ceux que l'on retrouve dans les registres publics tels que le registre des faillites et le registre des lobbyistes. S'il existe de bonnes raisons de rendre ces collectes accessibles au public – transparence et imputabilité – rares sont les bureaux d'enregistrement, s'il en est, qui contrôlent les détails des renseignements qu'ils communiquent ou les utilisations subséquentes de ces renseignements. Cette situation a donné lieu à des abus tels que la communication massive de renseignements personnels contenus dans les registres à des fins de marketing.

Le Parlement devrait apporter des modifications à la *Loi sur la protection des renseignements personnels* qui autoriseraient la communication de renseignements personnels contenus dans ces registres uniquement pour des raisons qui correspondent aux fins initiales pour lesquelles le registre a été établi.

Repenser les dispositions relatives à la communication

La démonstration la plus probante de la faiblesse de l'actuelle *Loi sur la protection des renseignements personnels* en ce qui a trait à la communication de renseignements personnels provient sans doute de la Cour d'appel fédérale, en 2000, dans l'affaire E-311 (*Le commissaire à la protection de la vie privée c. le procureur général du Canada*). La Cour a conclu que la disposition en matière de communication prévue à l'alinéa 8(2)b) de la *Loi sur la protection des renseignements personnels* habilitait le Parlement à conférer à n'importe quel ministre (par l'entremise d'un acte législatif) de vastes pouvoirs discrétionnaires en matière de communication de renseignements recueillis par le ministre dudit ministre.

Le commissaire à la protection de la vie privée a fait valoir que la *Loi sur la protection des renseignements personnels* oblige le ministre à communiquer les renseignements personnels uniquement aux fins pour lesquelles ils ont été recueillis ou pour un usage correspondant à ces fins. Toutefois, la Cour d'appel en est venue à la conclusion que

Il est vrai que toutes les améliorations à la Loi ne nécessitent pas de modifications législatives ; des directives administratives ou des directives relatives aux politiques peuvent souvent remplir ce mandat. En 1989, le Conseil du Trésor a fait part de lignes directrices présentant les démarches que les ministères devraient prendre avant de procéder au couplage de données, y compris la présentation d'une proposition détaillée à la commissaire à la protection de la vie privée aux fins d'examen. Compte tenu du peu de propositions de couplage de données qu'a reçues le Commissariat à la protection de la vie privée – et compte tenu que la pratique est vraisemblablement répandue – il est grand temps de prévoir des obligations à cet effet dans la Loi.

Limiter la collecte

Limiter la collecte est un principe fondamental de tout acte législatif régissant la protection de l'information. La *Loi sur la protection des renseignements personnels* oblige les institutions gouvernementales à recueillir uniquement les renseignements personnels « directement reliés » à un programme ou à une activité autorisé par le Parlement. Cela accorde au gouvernement une marge de manœuvre pour concevoir des programmes en ayant en tête un ensemble défini de renseignements personnels. Un contrôle plus rigoureux encore consisterait à exiger que les institutions démontrent que les renseignements sont *nécessaires* au programme ou aux activités.

Bien que le Conseil du Trésor interprète ainsi la *Loi sur la protection des renseignements personnels*, le Parlement devrait apporter des amendements à la Loi afin que ce sujet ne soit plus matière à interprétation.

Transparence gouvernementale

La *Loi sur la protection des renseignements personnels* oblige les institutions gouvernementales à informer les personnes pour lesquelles leurs renseignements personnels sont recueillis. Toutefois, cette mesure ne respecte pas vraiment le droit des personnes à exercer un contrôle sur la collecte, l'utilisation et la communication de leurs renseignements personnels.

Une explication plus éclairée et plus juste en regard des principes modernes en matière de protection des données devrait préciser :

- a) L'instance autorisée à recueillir les renseignements personnels ;
- b) L'utilisation possible des renseignements personnels ;
- c) les institutions auxquelles les renseignements personnels pourraient être communiqués ;
- d) si les renseignements sont discrétionnaires ou obligatoires ;

Toutefois, seules les personnes en territoire canadien ont le droit, en vertu de la *Loi sur la protection des renseignements personnels*, de demander l'accès aux renseignements personnels les concernant. Cela signifie que des passagers de transporteurs aériens outre-mer, ainsi que des personnes faisant une demande d'immigration, des étudiants étrangers et plusieurs autres étrangers dont les renseignements figurent dans les dossiers gouvernementaux canadiens, n'ont, selon la Loi, aucun droit d'examiner ces renseignements, de connaître la manière dont ils sont utilisés ou communiqués, ou de porter plainte auprès de la commissaire à la protection de la vie privée.

Il devient de plus en plus difficile de justifier une entrave au droit d'accès face à la mobilité internationale et à l'échange de données personnelles qui s'ensuit. Il ne semble pas non plus que cette entrave soit justifiée lorsque d'autres pays accordent le droit d'accès aux Canadiennes et aux Canadiens. Par exemple, la Directive européenne en matière de droit à la vie privée (à laquelle 25 pays membres se conformément) accorde le droit d'accès à « toute personne concernée » – c'est-à-dire toute personne dont des renseignements personnels sont détenus par une entité européenne.

La collecte de renseignements personnels de passagers par l'ASFC a mis en lumière les faiblesses de la *Loi sur la protection des renseignements personnels* et les difficultés à assurer un traitement équitable des renseignements personnels. Bien que l'ASFC ait accepté d'entendre administrativement ce droit aux citoyennes et aux citoyens qui ne se trouvent pas en territoire canadien, le groupe de travail de l'Union européenne et la commissaire à la protection de la vie privée préféreraient que tous se voient accorder l'accès en vertu de la Loi.

Contrôle efficace du couplage de données

Bien que l'usage que fait le gouvernement du couplage de données (ou « interconnexion des ordinateurs ») constitue vraisemblablement la plus grande menace à la protection de la vie privée des personnes, la *Loi sur la protection des renseignements personnels* reste silencieuse en ce qui a trait à cette pratique. Les commissaires à la protection de la vie privée (soutenus par les comités parlementaires) ont tous reconnu les dangers inhérents à la collecte excessive ou non justifiée de données. Tous ont fait la recommandation d'apporter des modifications à la *Loi sur la protection des renseignements personnels* afin de s'assurer que les institutions gouvernementales relient les dossiers personnels dans des systèmes discrets uniquement lorsqu'il est possible d'en démontrer la nécessité, et sous la surveillance permanente et vigilante de la commissaire à la protection de la vie privée du Canada. Ces recommandations n'ont pas été exécutées.

Protéger les renseignements non enregistrés

La technologie a démontré de façon éloquentes que le fait de limiter l'application de la *Loi sur la protection des renseignements personnels* aux renseignements personnels « enregistrés sous quelque forme que ce soit » est périlleux. La définition restrictive place les renseignements non enregistrés, tels que la surveillance électronique en temps réel (caméras de surveillance en direct) ou les échantillons biologiques, au-delà de la portée de la Loi. Pourtant, les technologies peuvent produire des données intelligibles au sujet de personnes identifiables qui devraient bénéficier d'une protection juridique.

Il est possible de modifier cette proposition; certaines lois provinciales régissant la protection des renseignements personnels et la *LPRPD* s'appliquent aux renseignements non enregistrés. Par exemple, une entreprise de sécurité des Territoires du Nord-Ouest et du Nunavut a installé quatre caméras de sécurité sur le toit de son édifice, l'objectif dirigé sur une des intersections principales de Yellowknife. Pendant plusieurs jours, 24 heures par jour, le personnel a visionné la transmission en direct et rapporté un certain nombre d'incidents à la police locale. Cette activité de surveillance visait à démontrer l'efficacité du service de l'entreprise et à mousser les affaires de celle-ci.

Bien que les protestations du public aient rapidement mis fin à cette démonstration, la commissaire était habilitée à enquêter et à émettre des conclusions en vertu de la *LPRPD*, laquelle fournit des conseils pratiques à d'autres organisations. La commissaire a conclu que même si la surveillance des places publiques était appropriée pour des raisons de sécurité publique, il faut d'abord en démontrer la nécessité, s'assurer qu'elle soit exécutée par les autorités publiques légitimes, et inclure toutes les mesures de protection licites en matière de protection de la vie privée.

Étendre le droit d'accès

La mondialisation signifie également que les institutions gouvernementales canadiennes détiennent maintenant des renseignements personnels concernant des ressortissants étrangers. Par exemple, l'ASFC recueille de l'information préalable sur les voyageurs/dossier passager pour les voyageurs venant au Canada. Les renseignements comprennent le nom, la date de naissance, la citoyenneté, le passeport ou le numéro de document de voyage, l'information sur la réservation et l'itinéraire du voyageur. Les transporteurs aériens recueillent les renseignements des passagers au point d'embarquement et les font parvenir à l'ASFC avant l'arrivée du vol.

Élargir la portée de la Loi sur la protection des renseignements personnels

Il n'y a pas que les années écoulées qui ont aveuglé la Loi sur la protection des renseignements personnels. Peut-être plus cruciale encore est la fonction de la loi, qui est de protéger les données plutôt que la vie privée en tant que telle. Bien qu'elle ait un certain mordant, la loi n'arrive pas, dans certaines circonstances, à faire mieux que d'« émettre des grognements ». La Loi est essentiellement un ensemble de vérifications et de contrepois au pouvoir gouvernemental. Elle prévoit une série de pratiques équitables de traitement de l'information pour régler les activités du gouvernement fédéral se rapportant à la collecte, à l'utilisation et à la communication de données personnelles concernant des personnes. Et la Loi donne à ces personnes le droit d'accès à cette information.

Étendre la juridiction

Il existe présentement des lacunes dans les champs d'application de la Loi sur la protection des renseignements personnels : plusieurs institutions, dont notre Commissariat, ne sont pas assujettis aux lois régissant la protection des renseignements personnels. Au fil des ans, le gouvernement fédéral a créé de nombreuses entités qui ne semblent ni assujetties à la Loi sur la protection des renseignements personnels ni à la LPPDE ; elles y échappent. Ces entités prennent la forme de conseils, de tribunaux, de commissions, de fondations, d'institutions et de corporations. Elles fonctionnent en association ou conjointement et sont financées par les gouvernements fédéraux et provinciaux. À notre avis, une telle situation affaiblit considérablement le contrôle qu'exerce le Parlement sur la protection des renseignements personnels. Pour le prochain exercice, nous avons entrepris une vérification afin de déterminer et de confirmer l'ampleur des lacunes, et d'évaluer les risques de façon plus détaillée. À ce jour, nous avons identifié plus de 30 entités qui ne sont pas clairement assujetties aux lois sur la protection des renseignements personnels.

Alors que le gouvernement crée de nouvelles institutions, un débat s'ensuit à savoir s'il faut ou non ajouter celles-ci à la liste des institutions visées. Compte tenu que le processus est malhabile et que le droit est suffisamment vital à une démocratie, il est permis de croire qu'il est justifié de donner préséance à la Loi sur la protection des renseignements personnels sur toute autre loi du Parlement. La Loi s'appliquerait donc à toutes les institutions fédérales à moins qu'une loi habilitante ou toute autre loi ministérielle ne déclare expressément qu'elle l'emporte sur la Loi sur la protection des renseignements personnels. Une disposition similaire apparaît déjà à la LPPDE.

services gouvernementaux en ligne. En fait, le succès du Canada en cette matière est remarquable. Selon une enquête annuelle sur la performance des gouvernements à l'échelle internationale, menée par Accenture, une entreprise offrant des conseils en gestion et des services technologiques, le Canada s'est hissé en première position parmi 22 pays pour la cinquième année consécutive. Offrir des services en direct aux Canadiennes et aux Canadiens est une priorité du gouvernement et devrait assurer moins de répétitions inutiles d'information et un meilleur service aux citoyennes et aux citoyens.

Toutefois, les demandes du cybergouvernement menacent de mettre fin aux silos de renseignements, lesquels fournissent leur propre protection structurée. Les silos de données sont peut-être contraires au concept de gouvernement en ligne ou cybergouvernement; il ne fait aucun doute qu'ils sont « moins efficaces ». Ils dupliquent les renseignements, et on ne peut pas se déplacer de l'un à l'autre.

En revanche, le cybergouvernement pourrait requérir des systèmes interopérables qui créent un bassin de renseignements personnels et mettent ceux-ci à la disposition d'un plus grand nombre d'utilisateurs à des fins plus nombreuses. Plus il y a de renseignements, de visites et d'utilisateurs, plus les personnes sont vulnérables à la surveillance excessive, qu'elle soit gouvernementale ou bureaucratique.

Sommes-nous en mesure d'accepter ce qui constitue en fait un fichier personnel détaillé et de faire confiance au gouvernement pour qu'il n'en fasse pas un usage inapproprié? Si oui, comment?

Le cybergouvernement procurera peut-être l'élan critique nécessaire pour faire de la *Loi sur la protection des renseignements personnels* un cadre de protection de la vie privée beaucoup plus efficace. La Loi doit établir des contrôles plus sévères d'accès au bassin de renseignements. Une meilleure loi exigerait une justification plus adéquate de la collecte de renseignements, *a priori*, par une justification clairement énoncée. Une meilleure loi exigerait également une adhésion plus rigoureuse au principe selon lequel les renseignements personnels doivent être utilisés uniquement pour les fins auxquelles ils ont été recueillis.

Le cybergouvernement est présent, mais la loi est toujours loin derrière. Si le gouvernement souhaite devenir le plus branché avec ses citoyennes et citoyens, il doit également assurer une plus grande protection de ces derniers.

Circulation transfrontalière des données

La *Loi sur la protection des renseignements personnels* doit aujourd'hui se débattre dans un monde où la « mondialisation » signifie bien plus que le commerce international de marchandises : la « mondialisation » signifie aussi une circulation à grande échelle de renseignements personnels à l'extérieur de nos frontières aux fins de traitement et de stockage par les gouvernements et le secteur privé. Dans les faits, cela signifie que les renseignements personnels quittent l'abri des lois canadiennes pour se retrouver dans un possible néant juridique.

Comme il l'a été mentionné plus haut, la communication de renseignements personnels d'un gouvernement à un autre a augmenté de façon régulière, en particulier depuis le 1^{er} septembre 2001 ; il en est de même pour la communication de renseignements par le gouvernement à des compagnies à l'étranger. Aucune disposition de la *Loi sur la protection des renseignements personnels* ne s'applique à des tiers situés outre-mer qui détiennent et traitent les renseignements personnels des Canadiennes et des Canadiens. Présentement au Conseil du Trésor, aucune politique ne régit les institutions gouvernementales en cette matière, même si certaines politiques sont à l'étude. Bien que nous accueillions favorablement les nouvelles politiques, le libelle de la *Loi sur la protection des renseignements personnels* devrait spécifiquement définir les responsabilités des instances qui communiquent les renseignements personnels à l'extérieur du secteur public et, bien entendu, à l'extérieur du Canada.

Une autre répercussion de l'impartition est que les renseignements personnels des Canadiennes et des Canadiens seraient mis à la portée de la *USA PATRIOT Act*, Comme le Canada et les États-Unis possèdent déjà moult ententes d'échange de renseignements à grande échelle à des fins d'application de la loi et de sécurité, on pourrait croire que les répercussions sur l'échange de renseignements et les dossiers du gouvernement sont faibles. Toutefois, si une institution ou entreprise canadienne décidait de traiter et de stocker des données sur ses clients aux États-Unis, les renseignements seraient alors à la portée des organismes américains, ce qui annulerait la protection fournie par la *Loi sur la protection des renseignements personnels* et la *LPRPD*.

Le gouvernement en ligne ou cybergouvernement

La *Loi sur la protection des renseignements personnels* doit également lutter contre la pression des organismes gouvernementaux – et le public, disons-le – pour fournir des

Cela aurait pu être évité. En 1987, trois ans après la mise en vigueur de la *Loi sur la protection des renseignements personnels*, le Parlement a procédé à l'examen prévu par la loi et a déposé un rapport détaillé recommandant que des modifications considérables soient apportées à la Loi. Dix ans plus tard, un autre comité parlementaire a recommandé qu'une révision importante soit effectuée. Les commissaires à la vie privée ont déposé une série de mémoires et de rapports, signalant les obstacles au droit à la vie privée des Canadiennes et des Canadiens que pose la technologie.

Les faiblesses sont encore plus manifestes lorsque nous comparons la *Loi sur la protection des renseignements personnels* – une loi de première génération sur la protection des données – à la nouvelle *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). En fait, on pourrait remédier à plusieurs préoccupations du Commissariat à la protection de la vie privée en adoptant des dispositions similaires à celles de la LPRPDE.

Le nouveau paradigme de la sécurité nationale

Tel qu'il a été mentionné plus tôt dans ce rapport, il semble qu'après les attentats du 11 septembre 2001 la sécurité nationale ait éclipsé tout le reste. Bien entendu, les Canadiennes et les Canadiens veulent assurer leur sécurité, ainsi que celle de leurs alliés. Comme toujours, le risque est que la grande expansion des systèmes de surveillance gruge de façon continue notre droit à la vie privée (entre autres droits), réduise nos attentes raisonnables en matière de protection de la vie privée et d'autonomie, et néglige la question cruciale qui consiste à savoir où s'impose la limite.

La *Loi antiterroriste* et la *Loi de 2002 sur la sécurité publique* ont toutes deux contribué à créer un environnement favorisant une plus vaste surveillance des personnes et des institutions. Une grande partie des renseignements de nature hautement sensible concernant la vie de personnes, de familles et de communautés est stockée dans des systèmes intégrés d'information auxquels les milieux chargés du maintien de l'ordre et de la sécurité ont facilement accès.

L'incidence cumulative des nouvelles lois est inquiétante. Premièrement, les pouvoirs de surveillance des organismes chargés de la sécurité et de l'application de la loi ont été exagérément élargis. Deuxièmement, les dispositions limitant l'usage de ces pouvoirs de surveillance – y compris par les tribunaux – ont été indûment réduites. Finalement, l'imputabilité et la transparence gouvernementales ont été considérablement réduites aussi. Nous prenons des risques en essayant de défendre notre société par des moyens qui abrogent les libertés fondamentales qui la définissent.

capteurs infrarouges détectant la chaleur, souvent sans que vous ne le sachiez ou sans votre consentement.

Les renseignements personnels sont devenus une marchandise lucrative. La protection de ces renseignements, en particulier dans le secteur public, est un défi continu pour les défenseurs de la protection de la vie privée – un défi d'autant plus difficile si l'on considère que la *Loi sur la protection des renseignements personnels* du Canada ne prévoit aucune mesure exécutoire de contrôle sur l'exportation de renseignements personnels.

Un long chemin

Dès les années 60, les Canadiennes et les Canadiens ont commencé à se questionner sur la relation entre les renseignements, la protection de la vie privée et le pouvoir politique. Ils ont commencé à craindre que l'usage croissant des ordinateurs n'entraîne la perte de l'individualité ou la conformité obligatoire.

En 1971, face aux préoccupations grandissantes, le ministère de la Justice et l'ancien ministre des Communications ont lancé un groupe de travail conjoint afin d'étudier les répercussions sociales et légales de la technologie informatique. De cette étude est né le rapport décisif *L'ordonnateur et la vie privée*. Les recommandations émises dans ce rapport ont mené, en 1978, à l'inclusion du droit à la vie privée dans la *Loi canadienne sur les droits de la personne*.

L'actuelle *Loi sur la protection des renseignements personnels* a été fondée sur ce droit et l'a renforcé. Elle reflète en plus les lignes directrices en matière de protection de la vie privée adoptées en 1980 par l'Organisation de coopération et de développement économiques (OCDE), dont le Canada est membre.

Le Canada est signataire de plusieurs instruments internationaux qui mettent l'accent sur l'importance ultime de la protection de la vie privée. *La Déclaration universelle des droits de l'homme* et le *Pacte international relatif aux droits civils et politiques* mentionnent tous deux le droit à la protection de la loi contre des impositions arbitraires dans la vie privée. La Cour suprême du Canada elle-même étouffe progressivement le droit à la vie privée par l'entremise de la *Charte canadienne des droits et libertés*. Mais face aux menaces du XXI^e siècle, la *Loi sur la protection des renseignements personnels* est désuète et souvent inadéquate pour protéger les données dans le secteur public.

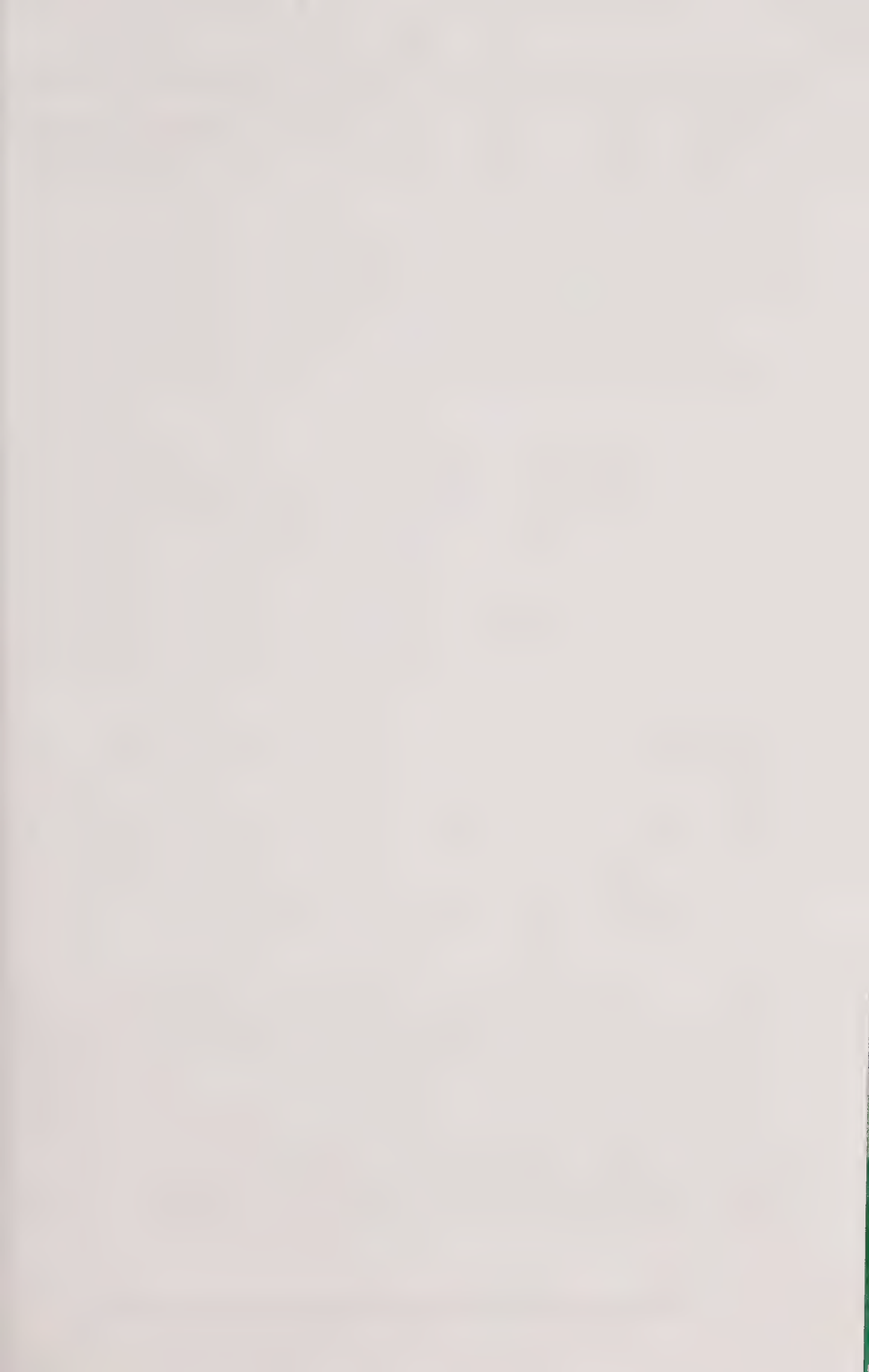
Réforme de la Loi sur la protection des renseignements personnels

Dans cette section, nous donnerons un aperçu de la situation et expliquerons certains éléments importants que le gouvernement doit prendre en considération pour actualiser la *Loi sur la protection des renseignements personnels*, c'est-à-dire pour entreprendre la réforme tant attendue.

Le tableau en matière de protection de la vie privée est infiniment plus complexe aujourd'hui qu'il ne l'était il y a dix ans. Face à la mondialisation croissante et à l'impartition à grande échelle du traitement et de la conservation des renseignements personnels, la *Loi sur la protection des renseignements personnels* du Canada fait preuve d'un retard déplorable.

Les technologies de l'information courantes de nos jours – Internet et les nouvelles technologies de surveillance telles que la vidéo numérique, les réseaux reliés, les systèmes de localisation mondiale, les boîtes noires dans les voitures, le dépistage génétique, les identificateurs biométriques et l'identification par radiofréquence – n'existaient pas au moment de l'entrée en vigueur, en 1983, de la *Loi sur la protection des renseignements personnels*. C'est un euphémisme que de qualifier la Loi de surannée quand il s'agit de faire face aux réalités d'aujourd'hui – il est plus juste de la comparer à un cheval de trait se démenant pour suivre des appareils technologiques frôlant la vitesse de la lumière.

De nouvelles technologies conçues pour surveiller les personnes ou capables de le faire, sont chose courante et ne sont pas réservées à l'usage des organismes chargés de l'application de la loi et de la sécurité nationale. Des entreprises, des personnes – même votre nouvelle voiture – recueillent des données personnelles par l'entremise de caméras de surveillance, de logiciels espions, de l'exploration de données et de



de renseignements personnels. Toutefois, nous devons nous assurer que les mesures prises en vue d'accroître la sécurité ne diminuent pas, en bout de ligne, les libertés qui définissent la société que nous défendons. Il nous faut des lois bien élaborées, une surveillance et une imputabilité accrue – et des mesures de contrôle et de contrepois efficaces.

Lorsque les droits sont restreints sans amélioration de la sécurité, tout le monde y perd. Par contre, l'accroissement de la sécurité sans érosion du droit légitime à la vie privée est une formule gagnante pour tous.

Bien entendu, les lois de la C.-B. ne protègent pas les renseignements personnels que le gouvernement fédéral transfère à l'extérieur du pays ; la *LPRPD* ne s'y applique pas non plus. Nous exhortons le gouvernement fédéral à étudier les circonstances dans lesquelles il permet aux renseignements personnels des Canadiennes et des Canadiens d'être traités à l'extérieur du Canada et d'expliquer aux Canadiennes et aux Canadiens la nature de ces transferts. La commissaire a fait valoir que « les Canadiens et les Canadiennes ont besoin de comprendre véritablement la mesure dans laquelle leurs renseignements personnels sont transférés par-delà les frontières, et la mesure dans laquelle les renseignements personnels qui les concernent peuvent être mis, et sont mis, à la disposition des gouvernements étrangers et des organisations étrangères ».

Au début de 2005, nous avons effectué un suivi en faisant parvenir une lettre au président du Conseil du Trésor exhortant le gouvernement à examiner l'incidence de l'impartition du traitement des renseignements personnels et à élaborer des clauses contractuelles protégeant les renseignements personnels communiqués à des tiers aux fins de traitement.

La vérification de l'Agence des services frontaliers du Canada

Nous avons également entrepris la planification de la vérification de l'Agence des services frontaliers du Canada (ASFC) qui se penchera sur l'échange de renseignements personnels avec les États-Unis. Les objectifs généraux de la vérification consistent à « évaluer la mesure dans laquelle l'ASFC contrôle et protège adéquatement la communication des renseignements personnels des Canadiens à des gouvernements étrangers ou à leurs institutions ». Un élément important sera l'établissement de rapports et de mises en correspondance, dans la mesure du possible, relativement aux renseignements des Canadiennes et des Canadiens que l'ASFC communique aux États-Unis et les raisons sous-jacentes.

La vérification permettra d'étudier plusieurs systèmes opérationnels importants que l'ASFC utilise pour traiter les renseignements personnels recueillis et échangés avec ses homologues américains. La vérification évaluera aussi la robustesse globale de la gestion de la protection de la vie privée à l'ASFC, et la façon dont celle-ci rend compte de ses responsabilités en matière de gestion de la protection de la vie privée au Parlement et au public.

En somme, la commissaire à la protection de la vie privée ne s'oppose pas à la lutte antiterroriste et à l'amélioration de la sécurité ; nous ne nous opposons pas à l'échange

d'assurance-médicaments. Les détracteurs de la proposition ont fait valoir que cela pourrait permettre à des organismes américains tels que le *FBI* d'obtenir, de l'entreprise américaine, les renseignements personnels des Canadiennes et des Canadiens en vertu de la *USA PATRIOT Act*.

En août 2004, nous avons présenté un mémoire au commissaire de la Colombie-Britannique intitulé « Communication transfrontalière de renseignements sur les Canadiens et les Canadiennes – Répercussions de la *USA PATRIOT Act* ». Le mémoire expliquait qu'une entreprise détenait les renseignements personnels de résidents canadiens vivant au Canada n'avait pas l'obligation de répondre à une ordonnance d'un tribunal afin de fournir ces renseignements à un gouvernement ou un organisme étranger, même si l'entreprise est une filiale d'une entreprise basée dans un pays étranger. En fait, l'entreprise contreviendrait à la *LPRPDE* si elle communiquait des renseignements personnels sans le consentement de la personne concernée. Seule une exception en vertu d'une loi donnée peut autoriser la communication de renseignements personnels, telle que les modifications apportées à la *Loi sur l'aéronautique* qui permettent aux transporteurs aériens de communiquer à un État étranger les renseignements qu'ils détiennent sur des passagers.

La *LPRPDE* prévoit une plus vaste protection et exige que les organisations qui communiquent des renseignements personnels à un tiers aux fins de traitement utilisent « un contrat ou autres moyens » afin de s'assurer que des entreprises situées à l'étranger procurent une protection des renseignements personnels comparable à celle du Canada.

Toutefois, le mémoire reconnaît que les entreprises détenant les renseignements personnels de Canadiennes et de Canadiens se trouvant à l'étranger doivent se conformer aux lois de ce pays et devraient communiquer les renseignements personnels s'il y avait une ordonnance de la cour. Cela signifie qu'une entreprise canadienne qui impartirait le traitement de renseignements personnels aux États-Unis exposerait de fait les renseignements aux lois américaines.

Le gouvernement de la Colombie-Britannique a réagi à la controverse en adoptant une loi modifiant la *Loi sur l'accès à l'information et la protection des renseignements personnels* (traduction libre) et neuf autres lois. Cette loi impose des limites aux organismes publics et aux fournisseurs de services de la Colombie-Britannique quant à la conservation et à la communication de renseignements personnels à l'extérieur du Canada, ainsi qu'à l'accès à ceux-ci.

avec les États-Unis. Par exemple, les deux pays ont mis sur pied des équipes intégrées de police des frontières et de police maritime, qui sont des organismes d'application de la loi, afin de coordonner leurs efforts dans la lutte contre les activités criminelles transfrontalières et terroristes.

Par contre, les Canadiennes et les Canadiens sont de plus en plus préoccupés par l'échange de renseignements personnels avec les États-Unis, particulièrement lorsque l'on tient compte du manque de surveillance de la part des organismes et des départements fédéraux américains sur la collecte, l'utilisation et la communication de renseignements personnels. De plus, la *Privacy Act of 1974* des États-Unis ne s'applique pas aux ressortissants étrangers, ce qui prive les Canadiennes et les Canadiens ainsi que les citoyens et citoyennes d'autres pays de certaines protections relatives aux renseignements personnels – dont le droit à l'accès et à la correction – en vertu des lois américaines. Lors d'un sondage des Associés de recherche EKOS, commandé par le Commissariat en mars 2005, 85 p. 100 des gens interrogés ont affirmé qu'ils étaient très ou modérément préoccupés par le transfert de renseignements personnels entre des organismes du gouvernement canadien et des gouvernements étrangers en vue de protéger la sécurité nationale.

L'incidence de la USA PATRIOT Act

Ces préoccupations ont été mises en évidence par une disposition de la *USA PATRIOT Act* (article 215), laquelle autorise un tribunal spécial à secrètement rendre une ordonnance obligeant « la production de toute chose concrète », dont possiblement les renseignements personnels d'une personne, au *Federal Bureau of Investigation* (FBI). La Loi interdit aussi à quiconque qui se voit signifier une telle ordonnance secrète de révéler s'y être conforme, ou même de révéler qu'une telle ordonnance existe.

En 2004, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidelis, a annoncé qu'il cherchait à savoir si la *USA PATRIOT Act* permettrait aux autorités américaines d'avoir accès à des renseignements personnels de la population de la Colombie-Britannique, par l'impartition des opérations du secteur public à des fournisseurs de services du secteur privé liés aux États-Unis qui en ont la garde ou le contrôle.

Le commissaire de la Colombie-Britannique a commencé l'examen à la suite d'une proposition selon laquelle une filiale canadienne d'une entreprise américaine se chargerait de l'administration des régimes provinciaux de soins médicaux et

L'Agence des services frontaliers du Canada (ASFC). Cette réorganisation entraînera l'intensification de l'échange de renseignements entre des entités autrefois distinctes.

Certains ont affirmé que la *Loi sur la protection des renseignements personnels* entraînerait la communication critique de renseignements personnels. La *Loi sur la protection des renseignements personnels* n'a pas besoin d'être modifiée en vue de faciliter l'échange d'information – cela est déjà possible. Elle doit l'être afin de contrer la surveillance accrue et la collecte ponctuelle de données à grande échelle que nous observons.

La réforme de la *Loi sur la protection des renseignements personnels* n'est pas une idée nouvelle. On la réclame depuis la fin des années 1980, bien avant la surveillance et les technologies de l'information d'aujourd'hui. Plutôt que de renforcer la Loi, le gouvernement en a affaibli les dispositions par des mesures telles que celles prévues dans la *Loi antiterroriste*.

Intégrer les systèmes d'information

L'investissement du gouvernement dans les systèmes intégrés d'information qui collectent et analysent une grande quantité de renseignements personnels sur nos habitudes de voyage, nos transactions financières et même, dans certains cas, sur les personnes que nous fréquentons, se fait de manière de plus en plus difficile à déceler. Les systèmes analysent et explorent les données personnelles en vue de repérer des modèles de comportement suggérant la possibilité qu'une personne présente un danger pour la sécurité, blanchit de l'argent ou finance un groupe terroriste.

Tandis que les organismes chargés de l'application de la loi et de la sécurité nationale recueillent davantage de renseignements, à partir de sources plus nombreuses, sur un plus grand nombre de personnes, le risque que des autorités prennent des décisions en se fondant sur des renseignements d'une exactitude douteuse ou pris hors contexte augmente. Les usages abusifs, les interprétations fautives et les communications inappropriées de renseignements personnels peuvent avoir des conséquences néfastes et préjudiciables pour les personnes, les familles, et même les communautés.

Le problème s'aggrave lorsque les dispositions de non-divulgation et le manque de transparence nous empêchent de déterminer à quel moment le système a failli et les raisons pour lesquelles une personne a été injustement ciblée.

Il n'est pas surprenant de constater que l'optique de la « frontière intelligente » en sécurité transfrontalière ait fait s'accroître la coopération et l'échange de renseignements

Plusieurs défis se posent pour la préparation de cet examen, dont celui d'essayer de déterminer si les pouvoirs extraordinaires que la *Loi antiterroriste* confère aux organismes chargés de l'application de la loi et de la sécurité nationale sont réellement nécessaires et efficaces. Nous n'avons trouvé aucune évaluation empirique de leur efficacité à détecter, à prévenir ou à dissuader les actes terroristes. Notre défi est plus grand encore : lorsque le gouvernement a accordé de nouveaux pouvoirs aux organismes chargés de l'application de la loi et de la sécurité nationale, il a également diminué la transparence et l'imputabilité.

La *Loi antiterroriste* ne peut pas être considérée seule. Au printemps 2005, nous avons exhorté les deux comités chargés de l'examen de la Loi à adopter une vision élargie de leur mandat afin d'examiner l'incidence cumulative sur le droit à la vie privée des Canadiennes et des Canadiens de toutes les mesures adoptées dans la foulée des attentats du 11 septembre – modifications à la *Loi sur l'aéronautique* (adoptées en fin d'année 2001), la *Loi sur la sécurité publique* et la *Loi sur l'immigration et la protection des réfugiés*.

Circulation transfrontalière des renseignements personnels

La *Loi antiterroriste* n'est nullement l'unique initiative du gouvernement qui menace la vie privée. Le gouvernement recueille, analyse et échange plus de renseignements personnels, avec le concours de la technologie, des nouvelles lois, de la réorganisation gouvernementale et d'une plus grande collaboration avec les États étrangers. La circulation de renseignements personnels entre les ministères et les organismes gouvernementaux a vraisemblablement augmenté de manière considérable, tant au pays qu'à l'extérieur du Canada.

Tous ces facteurs ont entraîné un changement fondamental dans l'équilibre entre la sécurité nationale, l'application de la loi et la protection des renseignements, et ont donné lieu à une diminution de la protection de la vie privée et des procédures équitables pour les personnes.

En avril 2004, le gouvernement du Canada a lancé sa tout première politique de sécurité nationale. La politique promettait la création d'un « centre d'évaluation intégrée des menaces » pour faciliter la collecte, l'analyse et l'échange de renseignements et d'autres informations. Le centre relève du SCRS, mais ses employés proviennent de plusieurs ministères et organismes.

Le gouvernement a subi une restructuration, d'où la création du nouveau ministère de la Sécurité publique et de la Protection civile Canada et de nouveaux organismes dont

s'appropriant celles-ci et en les mettant au service des forces de l'ordre, ce qui estompe dangereusement la démarcation entre le secteur privé et l'État.

Ce n'est pas seulement le secteur privé qui est intégré aux activités d'application de la loi ; la logique de la lutte antiterroriste s'impose également dans les initiatives plus conventionnelles en matière d'application de la loi et de sécurité publique. Cet état d'esprit menace d'éroder notre droit à la vie privée et nos autres libertés parce que les contraintes opérationnelles des organismes de sécurité nationale – par exemple, l'obligation d'obtenir une autorisation judiciaire – sont souvent plus faibles que celles régissant les organismes chargés de l'application de la loi.

Les débats sur la sécurité publique ne sont pas nouveaux. Ils ont cours depuis des années et remontent certainement plus loin que le 11 septembre. Toutefois, nous entendons aujourd'hui des messages explicites sur « les services de police axés sur le renseignement » et sur la vigilance comme moyens d'empêcher les terroristes de faire la loi dans notre société. Qu'il y ait prolifération de ces messages alors qu'il n'y a pas d'attention équivalente à l'égard de la nécessité de protéger les libertés civiles s'avère inquiétant. On observe maintenant une acceptation générale des divers types de surveillance et une dérive marquée vers une diminution de nos libertés civiles. Un État qui permet de façon régulière la présence de menaces à l'endroit des libertés civiles et du droit à l'autonomie consacré dans la Charte se retrouve en terrain glissant.

Si notre société se doit d'agir face aux préoccupations légitimes en matière de sécurité, nous devons aussi nous prémunir des marchands de peurs et de l'intolérance qui menacent une démocratie libérale.

Loi antiterroriste

La *Loi antiterroriste* (adoptée en automne 2001) requiert un examen parlementaire après trois ans. Le Sénat a nommé un comité spécial pour effectuer cet examen, tandis que la Chambre des communes l'a porté devant le Sous-comité de la Sécurité publique et nationale du Comité permanent de la justice, des droits de la personne, de la sécurité et de la protection civile.

En prenant part à cet examen, nous en formulons les questions les plus importantes, à savoir : les pouvoirs additionnels en matière d'application de la loi et de surveillance sont-ils nécessaires et proportionnels aux menaces qu'ils sont censés traiter? Les avantages en matière de sécurité qui en découlent justifient-ils le sacrifice de la protection de la vie privée et d'autres droits?

la vie privée s'est présentée à deux reprises devant des comités à ce sujet, d'abord devant un Comité spécial du Sénat procédant à l'examen de la Loi (9 mai 2005), ensuite devant un sous-comité du Comité permanent de la justice de la Chambre des communes (1^{er} juin 2005).

Afin d'agir efficacement à titre d'agent du Parlement, nous sommes d'avis qu'il faut entretenir de bonnes relations de travail avec les ministères et les organismes fédéraux. Le CPVP prévoit mettre davantage l'accent sur l'identification et la communication des préoccupations en matière de protection de la vie privée au moment où le gouvernement élabore certaines initiatives, plutôt que d'attendre qu'elles fassent leur entrée au Parlement, afin d'accroître les chances que ces préoccupations soient prises en considération.

Sécurité nationale

En mai 2004, le Parlement a promulgué la *Loi sur la sécurité publique*. Cette loi, présentée pour une première fois en novembre 2001 dans la foulée des attentats terroristes du 11 septembre, autorise le ministre des Transports, le commissaire de la Gendarmerie royale du Canada (GRC) et le directeur du Service canadien de renseignement de sécurité (SCRS) à demander aux transporteurs aériens et aux exploitants de systèmes de réservation de services aériens de leur fournir, sans mandat, certains renseignements relatifs aux passagers. Cette mesure peut paraître justifiée compte tenu des risques que représentent les terroristes pour le transport aérien, mais l'utilisation qu'en font les autorités n'est pas uniquement liée à la lutte antiterroriste ou à la sécurité des transports. La *Loi sur la sécurité publique* permet aussi d'utiliser ces renseignements pour identifier les passagers recherchés en vertu d'un mandat et pour un large éventail d'infractions criminelles ordinaires. En d'autres mots, les mesures de lutte antiterroriste servent à combler les lacunes de l'application ordinaire de la loi, nivelant par le bas le modèle généralement exigé des autorités responsables de son application.

Une autre disposition prévue dans la *Loi sur la sécurité publique* modifie la *LPRPDE* afin d'autoriser les organisations du secteur privé à recueillir des renseignements personnels sans le consentement du client et à les communiquer au gouvernement et aux organismes chargés de l'application de la loi et de la sécurité nationale. Les modifications ne s'appliquent pas uniquement aux sociétés de transport, mais à toutes les organisations assujetties à la *LPRPDE* – institutions financières, entreprises de télécommunications et détaillants. La communication de renseignements personnels sont une façon efficace de s'assurer le concours des organisations du secteur privé en

L'une des priorités de la dernière année a été d'améliorer notre façon d'évaluer, de surveiller et de prévoir l'activité parlementaire. Le CPVP a instauré un nouveau système amélioré pour suivre de près l'évolution des projets de loi au Parlement et pour rester à l'affût de nouveaux développements qui présenteraient un intérêt sur les plans de la promotion et de la protection du droit à la vie privée. L'objectif : ériger des ponts entre le CPVP et les ministères afin de leur faire part de nos observations plus tôt dans le processus législatif, au moment où nos commentaires peuvent être pris en compte de manière plus efficace. Lorsqu'un projet de loi a été déposé à la Chambre des communes, il est souvent trop tard pour repenser la façon d'aborder les enjeux en matière d'information.

Cette année, le Commissariat a répondu à une vaste correspondance et de nombreuses demandes de renseignements de sénateurs et de députés. La commissaire et les commissaires adjoints ont également rencontré en privé les sénateurs et les députés qui souhaitaient discuter de questions de politiques en matière de protection de la vie privée ou mieux connaître le fonctionnement du Commissariat.

Vers la fin de 2004, le CPVP a tenu, avec le Commissariat à l'information et en collaboration avec la Direction de la recherche de la Bibliothèque du Parlement, une séance d'information pour les parlementaires et leur personnel sur les rôles et les mandats des deux commissariats. L'assistance était nombreuse à la séance d'information et celle-ci a soulevé beaucoup de questions chez les participants. Nous sommes d'avis que de telles séances d'information contribuent à une plus grande sensibilisation aux enjeux relatifs à la protection de la vie privée sur la Colline du Parlement, et nous envisageons de tenir d'autres séances du genre à l'avenir.

► Priorités pour l'année qui vient

Le Commissariat prévoit une charge de travail élevée dans le domaine des affaires parlementaires pour le prochain exercice. De nombreux projets de loi d'intérêt pour le CPVP sont attendus au cours de la prochaine session, et l'examen parlementaire prévu par la loi de la Loi sur la protection des renseignements personnels et les documents électroniques doit débiter en 2006. Le CPVP prévoit jouer un rôle constructif au cours de cet examen en consultant judicieusement les parlementaires qui feront l'étude du fonctionnement de la Loi au cours de ses premières années de mise en application, et des modifications et améliorations possibles.

Le CPVP continuera de suivre avec intérêt l'examen parlementaire de la Loi antiterroriste. Au cours de l'exercice 2005-2006, la commissaire à la protection de

à la gestion et aux activités du Commissariat et une fois devant un comité sénatorial examinant les enjeux liés aux consommateurs dans le secteur des services financiers.

En 2004-2005, le CPVP s'est présenté devant des comités parlementaires traitant des projets de lois suivants :

- Projet de loi C-2, *Loi modifiant la Loi sur la radiocommunication* (6 mai 2004)
- Projet de loi C-12, *la Loi sur la quarantaine* (18 novembre 2004)
- Projet de loi C-22, *Loi constituant le ministère du Développement social et modifiant et abrogeant certaines lois* (9 décembre 2004)
- Projet de loi C-23, *Loi constituant le ministère des Ressources humaines et du Développement des compétences et modifiant et abrogeant certaines lois* (9 décembre 2004)
- Projet de loi C-11, *la Loi sur la protection des fonctionnaires dénonciateurs d'actes répréhensibles* (14 décembre 2004)
- Projet de loi C-13, *Loi modifiant le Code criminel, la Loi sur l'identification par les empreintes génétiques et la Loi sur la défense nationale* (8 février 2005)
- Projet de loi S-18, *Loi modifiant la Loi sur la statistique* (24 février 2005)

En ce qui concerne la gestion et les opérations du Commissariat, les représentants du CPVP se sont présentés devant les comités parlementaires en 2004-2005 pour discuter des sujets suivants :

- Rapport annuel et budget principal des dépenses 2003-2004 (17 novembre 2004)
- Budget supplémentaire des dépenses (1^{er} décembre 2004)
- Mécanismes de financement des agents du Parlement (10 février 2005)
- Rôle et fonctionnement du CPVP (16 février 2005)

► *Autres activités de liaison avec le Parlement*

Le CPVP a lancé plusieurs autres initiatives au cours de la dernière année dans le but d'offrir de meilleurs conseils au Parlement sur des enjeux en matière de protection de la vie privée.

En mai 2004, nous avons créé une fonction de liaison avec le Parlement afin d'améliorer nos relations avec le Parlement. Cette fonction relève de la Direction de la recherche et politique et reflète la volonté du CPVP de cibler ses activités parlementaires de façon à fournir aux députés et aux sénateurs des conseils éclairés et judicieux sur les politiques.

Guichet du Parlement pour la protection de la vie privée

A titre d'agente du Parlement, la commissaire à la protection de la vie privée relève directement du Sénat et de la Chambre des communes. Ainsi, le CPVP tient lieu de guichet du Parlement sur les questions de protection de la vie privée. Par l'entremise de la commissaire, des commissaires adjoints et des autres représentants du CPVP, le Commissariat porte à l'attention des parlementaires les enjeux ayant une incidence sur le droit à la protection de la vie privée des Canadiennes et des Canadiens. Pour ce faire, le CPVP dépose des rapports annuels au Parlement, se présente devant les comités du Sénat et de la Chambre des communes afin d'expliquer les répercussions des mesures législatives et des initiatives gouvernementales proposées sur la protection de la vie privée, et de dégager et d'analyser les enjeux qui, à son avis, doivent être portés à l'attention du Parlement.

Le Commissariat aide également le Parlement à être mieux informé en ce qui concerne la protection de la vie privée, en agissant à titre de ressource ou de centre d'expertise sur ces questions. À ce titre, il doit répondre à une vaste correspondance et à de nombreuses demandes de renseignements de sénateurs et de députés.

➤ *Présentations devant les comités parlementaires*

Les présentations devant les comités du Sénat et de la Chambre des communes constituent un élément clé de notre rôle de guichet du Parlement sur des questions de protection de la vie privée. Au cours de la période visée par ce rapport, la commissaire à la protection de la vie privée et les autres représentants du CPVP se sont présentés onze fois devant des comités parlementaires : six fois pour des projets de loi ayant une incidence sur la protection de la vie privée, quatre fois pour des questions ayant trait

Bien que la *Loi sur la protection des renseignements personnels* ne confère pas à la commissaire à la protection de la vie privée un mandat statutaire officiel de sensibilisation du grand public, la commissaire doit souvent informer celui-ci, ainsi que le gouvernement, en vue de s'acquitter de son mandat de responsabilisation des ministères et organismes du gouvernement fédéral en matière de traitement des renseignements personnels.

Notre mandat aux multiples facettes

Le Commissariat à la protection de la vie privée (CPVP) veille au respect de la Loi sur la protection des renseignements personnels à laquelle sont assujetties les institutions fédérales, et de la LPRPDE, qui régit le traitement des renseignements personnels dans le cadre des activités commerciales du secteur privé.

Le Parlement a investi le Commissariat du mandat de veiller à ce que le secteur public fédéral et le secteur privé (dans la plupart des provinces) rendent compte du traitement qu'ils font des renseignements personnels, et à ce que le public soit informé de son droit à la protection de la vie privée. Ce mandat n'est pas toujours compris.

En sa qualité d'ombudsman indépendant, le Commissariat agit à titre :

- *d'enquêteur* et de *vérificateur* possédant les pleins pouvoirs d'enquêtes et pouvant déposer des plaintes, mener des activités de vérification et s'assurer du respect des deux lois ;
- de *sensibilisateur du grand public* et de *défenseur*, ayant la double responsabilité de sensibiliser les entreprises à leurs obligations en vertu de la LPRPDE, et d'aider le public à comprendre son droit à la protection de ses données personnelles ;

- de *chercheur* et d'*expert* des enjeux en matière de protection de la vie privée auprès du Parlement, du gouvernement et des entreprises ; et

- de *défenseur des principes en matière de protection de la vie privée* dans les litiges ayant trait à l'application et à l'interprétation des deux lois régissant la protection des renseignements personnels. Nous analysons également les répercussions des projets de loi et des propositions gouvernementales sur les lois et les politiques.

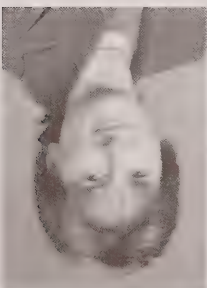
Cette année, nous publions deux rapports afin d'établir une distinction entre la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Cela nous semblait plus juste, compte tenu que la Loi sur la protection des renseignements personnels nous oblige à suivre l'exercice financier (2004-2005), alors qu'en vertu de la LPRPDE, nous sommes tenus de faire rapport en observant l'année civile (2004). De plus, chaque loi fournit un cadre distinct en ce qui a trait aux enquêtes et aux vérifications. Les deux rapports décrivent les efforts que nous avons déployés pour répondre aux attentes toujours plus nombreuses à l'égard du Commissariat pour que nous agissions, au nom du Parlement, à titre de gardiens de la protection de la vie privée des Canadiennes et des Canadiens. Les deux rapports se recoupent en plusieurs endroits, car un grand nombre de nos activités ne se rapportent pas spécifiquement à une loi ou à l'autre et, de plus en plus, les questions de politiques partagent des dénominateurs communs aux deux régimes.

Les Canadiennes et les Canadiens sont inquiets ; ils s'attendent à ce que nous appliquions la loi et à ce que le gouvernement respecte les valeurs inhérentes à notre constitution, comme le démontrent de récents sondages. Nous ferons notre part, mais la défense du droit fondamental à la protection de l'information repose sur un changement dans les politiques publiques, comme celui qui a été amorcé dans le domaine de l'environnement. Au cours des vingt dernières années, il est devenu évident que la pollution est néfaste, et l'habitude de recycler est entrée dans nos mœurs. La même prise de conscience doit se faire à l'égard des renseignements personnels : il est néfaste de recueillir des renseignements personnels sans consentement, de les communiquer avec indifférence, et de cacher au public les pratiques utilisées en matière de renseignements.

Trois thèmes principaux reviendront dans ce rapport, car ils constituent les enjeux les plus importants auxquels nous avons fait face : la sécurité et l'appétit démesuré pour les renseignements personnels et les mesures de surveillance qui ont surgi depuis le 11 septembre 2001 ; l'échange de renseignements et l'impartition du traitement des données outre-frontières et l'impératif de réformer la *Loi sur la protection des renseignements personnels*. Que vous lisiez ce rapport à titre de personne au sein du grand public, de fonctionnaire ou de parlementaire, nous avons un message à vous transmettre :

Il est grand temps de vous préoccuper de la protection de la vie privée avant qu'il ne soit trop tard. La participation des citoyennes et des citoyens au débat déterminera la direction que prendra notre pays en regard de la protection des renseignements personnels. Faites votre part pour contrôler la circulation des renseignements personnels de tous et chacun. Nous sommes là pour aider, mais nous ne pouvons accomplir la tâche seuls.

Avant-propos



Si la protection de la vie privée avait atteint sa pleine vigueur au Canada, les rapports annuels du Commissariat à la protection de la vie privée constitueraient un compte rendu détaillé d'interventions réussies pour défendre les droits des personnes, de vérifications d'institutions fédérales bien gérées, jouissant de processus opérationnels matures qui intègrent les exigences en matière de protection de la vie privée, et d'une analyse exhaustive de la politique sur les nouveaux systèmes d'information et les technologies. Dans la réalité, les rapports du Commissariat ont souvent donné l'impression d'une longue litanie sur la constante érosion de droits et l'assaut des nouvelles technologies de surveillance sur la vie des Canadiennes et des Canadiens, et notre impuissance à renverser cette tendance.

Ce ne sera pas différent cette année. Le phénomène de l'impartition et les associations public-privé nous portent de plus en plus à croire que le secteur privé détient des données sur les Canadiennes et les Canadiens, même lorsque celles-ci sont sous le contrôle du gouvernement.

De façon générale, nous sommes satisfaits des résultats de nos interventions, et de la coopération des entreprises et du gouvernement dans nos tentatives d'assurer le respect de pratiques équitables en matière d'information et des prescriptions de la loi ; mais les menaces à la protection de la vie privée semblent se multiplier tel un virus virulent qui pourrait prendre le dessus.

Si nous devons transmettre un message d'importance cette année, c'est que nous ne laisserons pas cela arriver. Nous sommes prêts, et nous comptons sur l'appui de toutes les institutions afin de nous aider à traiter ces enjeux, ainsi qu'à préserver et à maintenir la protection de la vie privée des personnes de ce pays.

Cadre de gestion de la protection de la vie privée.....	33
Elaborer un cadre de gestion de la protection de la vie privée à l'intention du gouvernement fédéral	33
Plaintes	39
Introduction	39
Enquêtes et demandes de renseignements	40
Plaintes reçues	40
Plaintes terminées	44
Définitions des conclusions en vertu de la Loi sur la protection des renseignements personnels.....	45
Processus d'enquête en vertu de la Loi sur la protection des renseignements personnels.....	51
Cas choisis en vertu de la Loi sur la protection des renseignements personnels.....	54
Incidents en vertu de la Loi sur la protection des renseignements personnels.....	64
Communication dans l'intérêt du public en vertu de la Loi sur la protection des renseignements personnels.....	66
Demandes de renseignements.....	67
Vérification et examen	69
Renforcer la fonction de vérification	69
Vérification de la circulation transfrontalière des renseignements personnels	70
Autres activités de vérification et d'examen	73
Devant les tribunaux	79
Recours judiciaires en vertu de la Loi sur la protection des renseignements personnels	79
Révision judiciaire.....	81
Sensibilisation du grand public et communications	83
Gestion intégrée.....	87
Vers le renouvellement institutionnel.....	87
Renseignements financiers.....	91

Table des matières

Avant-propos.....1

Notre mandat aux multiples facettes5

Point de vue de la politique7

 Guichet du Parlement pour la protection de la vie privée.....7

 Sécurité nationale.....10

Loi antiterroriste11

 Circulation transfrontalière des renseignements personnels12

 Intégrer les systèmes d'information.....13

 L'incidence de la *USA PATRIOT Act*.....14

 La vérification de l'Agence des services frontaliers du Canada.....16

Réforme de la *Loi sur la protection des renseignements personnels*19

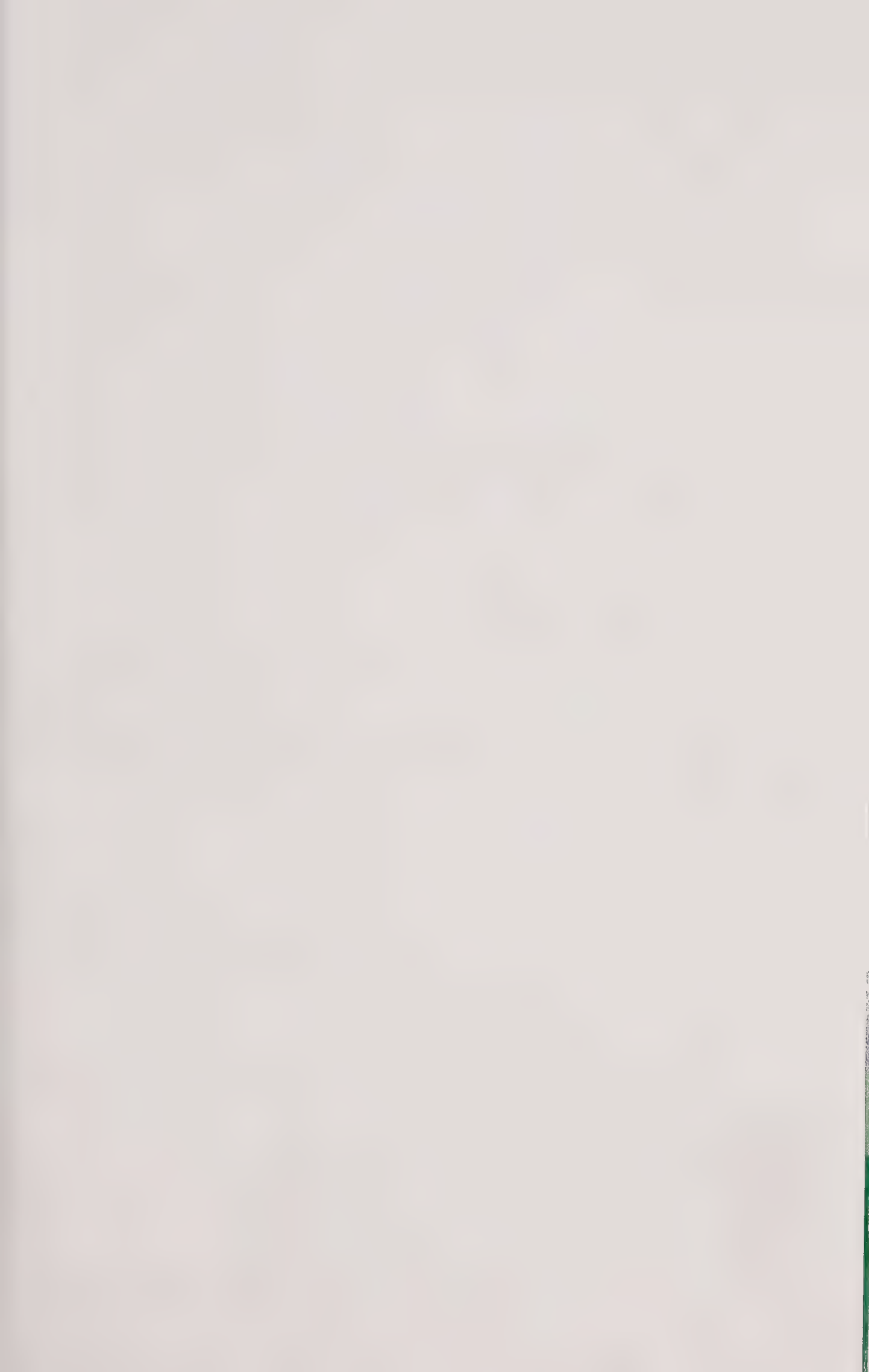
 Un long cheminement.....20

 Le nouveau paradigme de la sécurité nationale.....21

 Circulation transfrontalière des données.....22

 Le gouvernement en ligne ou cybergouvernement.....22

 Élargir la portée de la *Loi sur la protection des renseignements personnels*24



Octobre 2005

L'honorable Peter Milliken, député
Président
Chambre des communes
Ottawa
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2004 au 31 mars 2005 conformément à la *Loi sur la protection des renseignements personnels*.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

Jennifer Stoddart
Jennifer Stoddart





**Commissionnaire à la protection
de la vie privée du Canada
Privacy Commissioner
of Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télé. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tél. : (613) 995-8210
Fax : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



Octobre 2005

L'honorable Daniel Hays, sénateur
Président
Sénat du Canada
Ottawa
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2004 au 31 mars 2005 conformément à la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

Jennifer Stoddart
Jennifer Stoddart

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario) K1A 1H3

(613) 995-8210, 1 800 282-1376
Téléc. (613) 947-6850
ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 2005
N° de cat. IP50-2005
ISBN 0-662-68763-9

Cette publication est également disponible sur notre site Web à www.privcom.gc.ca, ainsi que le Rapport annuel concernant la Loi sur la protection des renseignements personnels et les documents électroniques 2004.

Canada

**Rapport annuel
au Parlement
2004-2005**
Rapport concernant
la Loi sur la protection
des renseignements
personnels

Vie Privée

Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada

Vie Privée

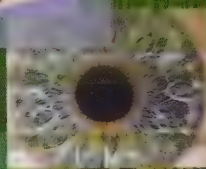
Commissaire à la protection
de la vie privée du Canada



Privacy Commissioner
of Canada

Rapport annuel au Parlement 2004-2005

Rapport concernant
la Loi sur la protection
des renseignements
personnels



Canada

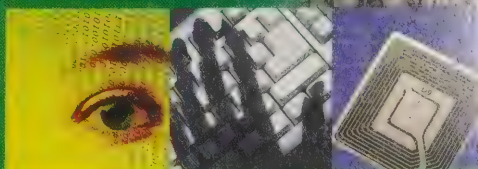
Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada

CA1
PC
- A573

Annual Report to Parliament 2005-2006



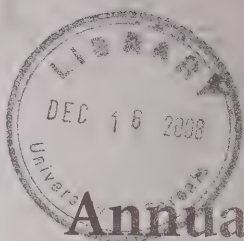
REPORT ON THE
Privacy Act

Canada

Privacy Commissioner
of Canada



Commissionnaire à la protection
de la vie privée du Canada



Annual Report to Parliament 2005-2006



REPORT ON THE
Privacy Act

Canada

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2006
Cat. No. IP50-2006
ISBN 0-662-49235-8

This publication is also available on our Web site at www.privcom.gc.ca.

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



June 2006

The Honourable Noël A. Kinsella, Senator
The Speaker
The Senate of Canada
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2005 to March 31, 2006.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

Foreword 1

Our Strengthened Mandate..... 5

Policy Perspective 9

 The Year in Parliament 9

Privacy Act Reform 12

 The Merger Issue 14

Policy Issues 17

 Public Interest Disclosures 17

 Transborder Data Flows 18

 International Liaison 20

 Radio Frequency Identification Devices (RFIDs) 21

 Videosurveillance Guidelines 21

 Identity Management and the War on Crime and Terror 21

Complaints..... 25

 Definitions of Complaint Types 25

 Definitions of Findings and other Dispositions under the *Privacy Act*. 31

 Findings by Complaint Type 32

 Complaint Investigations Treatment Times - *Privacy Act*. 35

 Select Cases under the *Privacy Act* 36

 Incidents under the *Privacy Act* 41

 Public Interest Disclosures under the *Privacy Act*. 45

 Investigation Process under the *Privacy Act*. 46

 Inquiries 48

Audit and Review	49
Stronger Privacy Management Framework Needed to Ensure Sound Privacy Management	49
Better Control and Accountability Required for Transborder Data Flow	52
Our Key Findings	54
Importance of Privacy Impact Assessments	55
Other Work	60
In the Courts	61
<i>Privacy Act</i> Applications	61
Judicial Review	62
Public Education and Communications	65
Public Opinion Polling	65
Speeches and Special Events	66
Media Relations	66
Web Site	66
Publications	66
Internal Communications	67
Corporate Services	69
Planning and Reporting	69
Human Resources	69
Finance and Administration	70
Information Management / Information Technology	71
Our Resource Needs	71
Financial Information	71
Appendix 1	73
Appendix 2	77

FOREWORD

Next year will be the 25th anniversary of the *Privacy Act*, Canada's first comprehensive privacy legislation. Revised from the 1977 part IV of the *Human Rights Act*, which recognized the basic principles and established a Privacy Commissioner who was a member of the Human Rights Commission, the *Privacy Act* was framed in the kind of thinking we had about government in the 1960s and 1970s. We worried about big central databases, run on huge mainframe computers. We talked about files, and we thought of records systems as paper files in filing cabinets. All that was before the personal computer, the Internet and powerful search engines like Google. Public servants did their work on paper, armed with typewriters filled out forms in triplicate.



Why am I wandering down memory lane? Because the world has changed in ways that are profound, and deeply troubling from the perspective of individual privacy and human rights. When we imagined powerful central computers which could impact privacy, armed with the new social insurance number to secure reliable matches, we lived in a world that was strictly bounded by capacity... the limited capacity to store data, the limited capacity to match data, the limited capacity to move data around and expose people to risk of privacy breaches. The Office of the Privacy Commissioner was designed as a small agency, with very limited powers, and Treasury Board Secretariat and the Department of Justice were tasked with implementing the new legislation and helping public servants to interpret it.

Now we live in a world that is strictly bounded by our capacity to understand it, by our ability to keep up with the pace of technological change, and to manage the new risks and security challenges that come with limitless storage capacity, limitless

transmission capacity, limitless data mining capacity. We are bounded by our own limited capacity to understand, to imagine the implications of data flow and data aggregation, and our ability to teach. The challenge of protecting data is increasingly globalized, because actions in one distant part of the world now may directly impact the privacy of Canadians. A spammer sending unwanted e-mail with spyware from somewhere in Eastern Europe can cause havoc in a Canadian internet service provider, wiretaps to detect anything from terrorism to money laundering are global in scope and application, and Canadian travellers need identity documents and financial instruments that will help them establish credentials as they do business around the world. Life is complicated, and so is privacy in today's world.

We need to understand the implications of countless new information systems, new laws and regulations, new systems of surveillance which are being constructed in the name of public safety. We need to audit more of these applications, to bring earlier insight and assistance to government departments who have a myriad of complex decisions to make and may not be as well versed in privacy matters as we are. We are determined to move forward with new resources and further enhance our ability to provide advice and assistance to Canadians, to Parliament and to the many public servants who are working to improve life for Canadians.

But at the risk of sounding like *Oliver Twist*, I want to say "Please sir, can I have some more?" It is my sincere hope that we can celebrate the federal public sector privacy law's anniversary with the knowledge that Parliament will give us a new *Privacy Act*. We need one that can respond to the age of information, to the challenges of ambient computing, to the reality of huge government systems that are capable of a surveillance we could not have dreamed of in 1982. Poll results suggest that more than 70% of Canadians have a high sense of erosion of their privacy and the protection of their personal information, and predict that it is one of the most important issues facing the country.

Canadians deserve real redress when things go wrong, not a Privacy Commissioner who has no power to even take a wrongful collection or a shameless disclosure of personal information to the Federal Court for a judgment and damages. We had started down a path of providing rights for Canadians in 1982, and we went a step further with the coming into force of the *Personal Information Protection and Electronic Documents Act* for the private sector in 2001, but we must now go further and ask our government to meet the standards that the power the information age demands. It is not acceptable that the standards for privacy protection are higher for the private sector than they are for the public sector.

We are proud to be hosting the International Conference of Data Protection and Privacy Commissioners in the fall of 2007 in Montreal. More and more, other countries, many of which will be attending this important event, are looking to Canada as a model for data protection. As an illustration of the interest other countries have in our data protection regime, we have had professional development activities with the authorities in Mexico, France and the U.K. Canada must keep its place as a leader in this area, and in my view this requires an update of the public sector law. It is simply not acceptable that we have higher standards for privacy protection in the private sector.

Real privacy demands a real balance of power between the citizen and the state, with real oversight and real power to intervene. We can do it, and we are anxious to get on with the real work it entails. As we committed, we have recently tabled with the Standing Committee on Access to Information, Privacy and Ethics our recommendations for amendments to the *Privacy Act* shortly, and we look forward to a fruitful dialogue.

Since my appointment as Privacy Commissioner in December of 2003, and certainly in the past fiscal year, my focus and that of my team has continued to be the institutional renewal of this Office. Rebuilding the Office had to take precedence. We also devoted our energies last year to a Business Case for long-term, stable funding, which involved an independent review of our activities and a presentation to a special Parliamentary Panel for their recommendation. I am pleased to report that the Office has now turned the page. We are moving forward with renewed vigour. We will continue our collaborative efforts with our provincial and territorial counterparts, as well as with our international colleagues, so that we can truly take on the significant privacy challenges ahead.

OUR STRENGTHENED MANDATE

Our Office is responsible for overseeing compliance with both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. Although they are two separate laws, we manage the resources as a single pool. To date, our Office has not received permanent funding to carry out its duties under *PIPEDA* and the funding level for the *Privacy Act* has remained unchanged for many years. Funding for *PIPEDA* was granted for three years only. *PIPEDA* came into force in stages, beginning in 2001 and reaching full implementation in 2004, and we thought it important to let the dust settle before we attempted to identify long-term financial needs. *PIPEDA* has now been in full force for two years, and the demands made of us under both laws are increasing.

Funding levels for the administration of both Acts left us unable to carry out our multi-faceted mandate. We now have a significant backlog of complaints particularly under the *Privacy Act*, and complainants are, quite understandably, becoming impatient. The small size of our team of auditors makes it impossible to conduct effective audits to ensure compliance. Even though we have adopted a risk-based approach, we need to intensify our audit activities. Funding limits also mean that our communications strategy has been primarily reactive, when proactive public education about privacy rights and obligations is required instead. Similarly, our Policy and Research Branch and our Legal Services Branch have been confined to putting out existing privacy fires, rather than anticipating and therefore more effectively addressing emerging privacy issues.

In the past few years, the Office went through an extremely challenging period. However, every cloud has a silver lining. In this case, the silver lining was an opportunity to review the functioning of the Office, in detail, from top to bottom. The result is an Office of the Privacy Commissioner of Canada that is pointed in the

right direction. It is now time to put forward the Office's new vision and we need the full set of tools to implement it.

We are attracting new and highly specialized talent to our team. We have pursued an ambitious agenda to correct deficiencies in management of the organization. Audits and evaluations of our Office – by the Auditor General of Canada, the Public Service Commission and the Canadian Human Rights Commission – have so far been positive. And we have implemented a thoughtful, systematic process to determine our organizational needs. This Office is a stable institution worthy of the trust of Parliament and the Canadians it serves.

The Vision of the Office of the Privacy Commissioner of Canada

The Office has prepared two analyses of significance – a Vision and Institutional Service Plan, and a Business Case for Permanent Funding. Together, these describe who we need to be, for Canadians and on behalf of Parliamentarians, and what it takes to get us there.

If funded appropriately, the Office can accomplish the following in relation to the activities regulated under the *Privacy Act* and *PIPEDA*:

- undertake a meaningful number of audits and reviews to encourage greater compliance, and assist in developing a robust privacy management regime;
- work with government institutions, and conduct legal and policy analyses of bills and legislation to assist Parliament;
- make more proactive, extensive and effective use of the enforcement tools entrusted to us by Parliament, including Commissioner-initiated complaints, court actions and public interest disclosures;
- carry out research into emerging privacy issues and trends to help citizens and policy makers understand current and future privacy challenges;
- engage in public education to better inform individuals of their rights, and organizations of their obligations;
- through a streamlined investigation process, tackle the growing backlog of privacy complaints; and, finally,
- sustain institutional renewal efforts.

Business Case: Resources

This past year, our Office was pleased to take part in an innovative and entirely new process for seeking funding approval for the operations of Officers of Parliament. We embraced the opportunity to engage Parliament in a constructive dialogue about our

funding needs. But before doing so, we certainly did our homework. Our Vision and Institutional Service Plan and our Business Case for Permanent Funding provided a comprehensive framework for protecting the privacy rights of Canadians and residents, and for serving Parliament in meeting its needs for privacy expertise as it considers legislation. The Service Plan and Business Case are the Office's blueprint for a stronger and more effective institutional role.

Parliamentarians agreed with this vision. The new House of Commons Advisory Panel on the funding of Officers of Parliament was supportive of our request for funding. The Office will now be in a better position to serve Canadians with close to a 50% increase in human and financial resources. At the end of 2005-2006, on which we are reporting, we planning for that increase within the next two years.

POLICY PERSPECTIVE

The Year in Parliament

2005-06 has been a busy year in Parliament for the Office. A key component of the work we do involves appearing before Committees of the Senate and House of Commons to provide our expert advice on the privacy implications of bills and other policy matters under consideration by Parliament.

The Office was called on to appear before Parliamentary Committees a total of eleven times in fiscal year 2005-06 (sixteen times in calendar year 2005). For a small organization such as our own, this represents a considerable amount of work, but because the Privacy Commissioner is an Officer of Parliament it is central to our mandate. Ten of these eleven appearances were on bills and policy issues that fall under the purview of the *Privacy Act*, although some appearances, such as those on funding, also pertain to the *Personal Information Protection and Electronic Documents Act*.

Bill S-18, *An Act to Amend the Statistics Act*. (Before the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology.)

- This enactment removes a legal ambiguity in relation to access to census records made between 1910 and 2005. It allows unrestricted access to those records, beginning 92 years after the census was taken. Starting in 2006, the consent of Canadians is required in order for their census information to be released 92 years after the census is taken. The OPC did not oppose the release of census records after 92 years and would be pleased to see consent provisions included in the Act, noting that Canadians should have the right to decide for themselves if they want their personal census records to be made publicly available in the future. The bill came into force when it received Royal Assent on June 29, 2005.

- Bill C-37, *An Act to Amend the Telecommunications Act*. (Before the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology.)

This enactment aims to reduce the volume of unsolicited telemarketing calls Canadians receive at home by providing the Canadian Radio-television and Telecommunications Commission (CRTC) with the ability to establish a national Do Not Call List (DNCL). Under the legislation, the CRTC has the power to levy substantial penalties against telemarketers who do not follow the rules. The OPC expressed its strong support for the general intent underlying this bill when it was first introduced in Parliament. However, Bill C-37 also sets out a list of telemarketers who are exempt from the CRTC's requirements or prohibitions in relation to a national DNCL. The OPC expressed opposition to the inclusion of these exemptions. We suggested instead that the House of Commons delay the inclusion of any exemptions until such a time as Parliament had more fully consulted with Canadians on the matter, as was originally recommended by the then minister responsible for the Bill. This advice was supported by the majority of our provincial counterparts. Nevertheless, Parliament decided to incorporate exemptions. Bill C-37 received Royal Assent on November 25, 2005, and will come into force on a day to be fixed by order of the Governor in Council.

- Bill C-16, *An Act to Amend the Criminal Code (impaired driving) and to make consequential amendments to other Act*. (Before the House of Commons Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness.)

This enactment amends the Criminal Code to clarify that the reference to impairment by alcohol or a drug in paragraph 253(1)(a) of that Act includes impairment by a combination of alcohol and a drug. It authorizes specially trained peace officers to conduct tests to determine whether a person is impaired by a drug or a combination of alcohol and a drug and also authorizes the taking of samples of bodily fluids to test for the presence of a drug or a combination of alcohol and a drug in a person's body. The OPC expressed support for the intent of the legislation, which is to make our roads safer and to protect Canadians against the effects of impaired driving. However, we had some concerns about the way in which the Bill proposed to address the problem. In particular, these concerns related to the effectiveness and the proportionality of the measures that were being proposed. One of the fundamental principles of fair information practices underlying the *Privacy Act* is that personal information should not be collected unless it can be used

to achieve the specific purpose for which it has been collected. Forcing people to provide bodily fluids is intrusive; the intrusion is compounded when the samples cannot, with confidence, be used to measure impairment. Nevertheless, we noted that if, despite these concerns, the government decided to move ahead with the legislation, provisions needed to be made to ensure that the bodily fluids collected and the results derived from tests were adequately protected. Bill C-16 died on the Order Paper at committee report stage.

- Review of the *Anti-terrorism Act*. (Before the Senate Special Committee on the *Anti-terrorism Act*, and the House of Commons Subcommittee on Public Safety and National Security.)

The *Anti-terrorism Act* received Royal Assent on December 18, 2001. It amended the *Criminal Code*, the *Official Secrets Act*, the *Canada Evidence Act*, the *Proceeds of Crime (Money Laundering) Act* and a number of other Acts, and enacted the *Charities Registration (Security Information) Act*, in order to combat terrorism. In 2005, a House Committee and a Senate Committee both independently undertook a comprehensive review of the Act, as mandated by the legislation to take place three years after it received Royal Assent. The OPC appeared before both Committees reviewing the legislation. Our remarks focused primarily on the lack of facts and evidence to suggest that the measures provided for by the *Anti-terrorism Act* are necessary. We also urged the Committees to critically assess the issue of proportionality and to consider a number of practical recommendations proposed by our Office to address the cumulative impact of anti-terrorism measures on the privacy rights of Canadians.

A key Committee for the Office is the relatively new Standing Committee of the House of Commons on Access to Information, Privacy and Ethics (ETHI). Established in late 2004, this Committee is significant in that with its creation, Canadians now have a Standing Committee of the House of Commons dedicated to privacy matters. The Privacy Commissioner of Canada and other OPC officials appeared three times before the ETHI Committee in 2005-06. While a common reason for these appearances was to question us on the operations of our Office through examination of our Estimates and Annual Reports, Members of the Committee also had many questions and concerns regarding some of the key privacy challenges and opportunities facing Canadians. The OPC looks forward to a continued, productive working relationship with this Committee in the 39th Parliament. As privacy issues continue to grow in number and complexity, it is vital that Parliament have a focus to examine these issues and reflect on the concerns expressed by Canadians.

Finally, a new House of Commons Advisory Panel on the Funding for Officers of Parliament was created this year. The new Panel was responsible for assessing and making recommendations on the OPC request for additional resources. The OPC appeared twice before this Panel to present its Business Case.

Privacy Act Reform

Recommendations for reform of the *Privacy Act* have been made ever since the first legislated review, which resulted in the 1987 report of the Standing Committee on Justice and Solicitor-General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. Despite the fact that the report, containing more than 100 recommendations, was unanimously supported by members of the Committee, none of the recommended changes have been enacted, although, in its response, the government committed to move on amendments by the fall of 1988.

In his last report, for 1999-2000, then-Commissioner Bruce Phillips pointed out that Parliament had not turned its mind to the *Privacy Act* in 14 years, although numerous recommendations had been made during the 1990s by the Privacy Commissioner. He called the weaknesses of the *Privacy Act*

“... all the more striking now that Parliament has passed the *Personal Information Protection and Electronic Documents Act*. This act (which regulates personal information handling in the private sector) contains many features that are superior to the *Privacy Act*, making a comprehensive review of the existing law both urgent and unavoidable.”

A detailed review of the Act, *Privacy Act Reform: Issue Identification and Review*, was completed by this office in December 1999, released in June 2000 and submitted to the Department of Justice in anticipation of that “urgent and unavoidable” review.

That review has yet to take place.

Canadians have become much more familiar with the privacy protection principles underlying the private sector law and no doubt expect that personal information in the hands of the government has at least as much protection as personal information in the hands of businesses. If the review of the Act was “both urgent and unavoidable” in 2000, it is even more so today.

To that end, the latest report produced by this Office focuses on the obligations of government institutions. This report was prepared at the invitation of the Standing Committee on Access to Information, Privacy and Ethics, an invitation extended when the OPC appeared before the Committee last fall to discuss our annual reports for 2004-05. *Government Accountability for Personal Information: Reforming the Privacy Act* was recently submitted to the Committee.

The *Privacy Act* was introduced as, and should remain, to the extent possible, the companion of the *Access to Information Act*. The new government has made accountability a centerpiece of its mandate and it is our hope that the long-postponed review and amendment of the *Privacy Act* will finally take place. In preparing *Government Accountability for Personal Information*, our Office has been informed by the proposals for reform presented to the Committee by the Information Commissioner in September 2005 and the report of the Special Advisor to the Prime Minister, Mr. Gérard La Forest, submitted in November.

Since the *Privacy Act* came into being over 20 years ago, the privacy landscape has become much more complex. Technological and social changes in the last 20 years – the creation of the Internet and the World Wide Web, new information and communication technologies, globalization, global positioning systems, video surveillance, outsourcing, data mining and the commodification of personal information – have not just changed the landscape, they have put us on another planet.

As a quasi-constitutional statute, the *Privacy Act* must have primacy over other legislation, except in the most exceptional circumstances. All federal government institutions must be subject to the *Privacy Act* – not just departments and agencies. Officers of Parliament, Crown corporations, the various Foundations set up in recent years, and other entities which carry out important functions related to public health and safety must also be subject to the *Privacy Act*. Any person, not just Canadian citizens or other persons present in Canada, must have the right to apply for access to their personal information held by a Canadian government institution. The definition of personal information must, in this technological and digital age which permits real-time surveillance, include unrecorded as well as recorded information about an identifiable individual. In addition, a person must be able to challenge in court not just a refusal of access to their personal information, but also inappropriate collection, use or disclosure of that information.

The Privacy Commissioner must have as broad a mandate under the *Privacy Act* as it does under the private sector legislation, including the power to use mediation and conciliation to resolve complaints, to conduct research on privacy-related issues, and to educate the public and government institutions about their rights and obligations. The duties of government institutions concerning collection, use and disclosure of personal information must be more clearly specified. Important policies for achieving the goals of the *Privacy Act* have been developed by Treasury Board. These obligations respecting data matching, the management and security of government information, the establishment of privacy management frameworks, the conduct of privacy impact assessments for new programs and guidance for protecting privacy in outsourcing contracts should have the authority of legislation behind them. Without such authority, these policies remain exposed to the vagaries of executive government.

To increase accountability and transparency of government institutions with respect to personal information, reporting requirements need to be strengthened and Parliamentary committees need appropriate support and resources to review the personal information practices of government institutions, as well as their performance of *Privacy Act* responsibilities. Institutions must remain accountable for personal information they are permitted to collect, even though it may be collected or processed by others, especially by contractors outside of Canada.

Although not within this reporting period, it is important to note the new government's *Federal Accountability Act*, introduced April 11, 2006. This bill includes the first set of proposed amendments to the *Access to Information Act*, with parallel amendments to the *Privacy Act*. These amendments extend the scope of the Acts to include additional Crown corporations and the Officers of Parliament (including this Office). The government has further confirmed its commitment to move ahead with comprehensive reform of the *Access to Information Act*. This will necessarily require consideration of the parallel provisions in the *Privacy Act*. It is our hope that this will be the year the government finally carries out the "urgent and unavoidable" review and updating of the *Privacy Act*, not just concerning issues in common with the access legislation, but also including the broader range of issues addressed in *Government Accountability for Personal Information: Reforming the Privacy Act*.

The Merger Issue

In July 2005, former Supreme Court of Canada Justice, the Hon. Gérard V. La Forest, was appointed as a special advisor to the Minister of Justice to assess the merits of merging the offices of the Information Commissioner and the Privacy

Commissioner into a single office. Mr. La Forest was also to examine the merits of cross-appointing a single Commissioner to both functions while maintaining two separate Commissions.

A shift in the structure of dealing with access to information and privacy issues at the federal level could have implications on several fronts, not the least of which was the quality of protection of the privacy rights of Canadians.

In our formal response, delivered to Mr. La Forest in October 2005, we concluded that this is not the appropriate time to consider merging the two offices. In reaching this conclusion, we noted the general lack of scholarly literature on the merits and problems associated with either a “twinned” model or the current federal model. The decision to move towards a particular model must necessarily be based more heavily on assumptions than on a historical record.

We also cautioned that the discussion about the potential framework for asserting access to information and privacy rights at the federal level should not detract from other important concerns affecting these rights. Among those concerns were an appropriate legislative framework, adequate resources to fulfill legislated functions, and a broad mix of tools and processes to foster a culture of compliance that shows respect for the values represented by privacy and access laws. We argued that a review of privacy and access to information legislation was paramount and should precede the discussion of organizational models. The important issue was perhaps not the shape of the container surrounding privacy and access to information, but the quality of the product inside.

In his November 15, 2005, report, Mr. La Forest stated that the burden of persuasion lies with those advocating a merger of the offices of the Information and Privacy Commissioners or a cross-appointment of a single commissioner to both offices. He concluded that this burden had not been met. Each of the one- and two-commissioner models has advantages and disadvantages, he concluded, and in the abstract, neither is demonstrably superior to the other. “But considering the unique features of the federal access to information and privacy environments, and the investments that interested parties have made in the existing structure, moving to a single commissioner model would, in my estimation, have a detrimental impact on the policy aims of the *Access to Information Act*, the *Privacy Act*, and the *Personal Information Protection and Electronic Documents Act*.”

POLICY ISSUES

Public Interest Disclosures

Protecting personal information from unwarranted disclosure is an ongoing task for this Office. However, there are circumstances when personal information held by government institutions can and should be disclosed, even without the consent of the person to whom the information relates. Certain disclosures in the public interest fall into this category.

The *Privacy Act* allows for “public interest” disclosures of personal information in limited circumstances. Section 8(2)(m) of the Act permits “disclosure of personal information without the consent of the individual where, in the opinion of the head of the institution:

- the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or
- disclosure would clearly benefit the individual to whom the information relates.”

This provision has been used, for example, to make public details about an individual who is being released from custody and who poses a threat to the community.

The head of the institution decides whether the public interest outweighs the right to privacy. The institution must notify the Privacy Commissioner that it will be disclosing personal information in the public interest. The Commissioner may express concerns with the proposed disclosure and may, if she thinks it appropriate, notify the individual whose information will be disclosed. However, the decision to release the information in the public interest, and how much to release, rests solely

with the head of the institution. The Privacy Commissioner has no authority to prevent the disclosure.

The *Privacy Act* is therefore abundantly clear about allowing public interest disclosures. Unfortunately, the public disclosure provision is not well understood and, on occasion, the Act is perceived as standing in the way of safety and security by blocking the release of personal information. Too often we hear representatives of government institutions arguing that the *Privacy Act* prevents them from releasing personal information, when in fact the head of the institution could release the information in the public interest. This inaccurate explanation of the role of the Act wrongly paints the Act as the villain.

We do have some sympathy for the predicament facing government institutions on this point. In some situations – for example, following a natural disaster or crime – a reporter may confront a spokesperson for the institution and ask for the name and other personal information about a victim. The spokesperson may simply err on the side of caution and refuse to release that information.

We have no quarrel with this caution, since the spokesperson has no authority under the *Privacy Act* to order the release of the personal information in the public interest, and the decision to release should not be taken lightly in any event. Only the head of the institution or the head's delegate can make the decision to release information in the public interest. In many cases, the information will later be released, but only after the head of the institution has decided that the release is appropriate.

Our concern lies instead with the simplistic characterization of the *Privacy Act* as the barrier to disclosure. It would be more appropriate, and a more accurate interpretation of the *Privacy Act*, for the spokesperson to say that the authority to release personal information rests with the head of the institution, not with the spokesperson. We encourage government institutions to remind spokespersons to respond in this manner when pressed for personal information.

Transborder Data Flows

Last year we wrote about the concerns registered in Canada about the impact of the *USA PATRIOT Act* on data held by US based companies. The *USA PATRIOT Act* has become the symbol of the increasing concern of Canadians about the security of their personal information when it leaves Canada. The *USA PATRIOT Act* was passed rapidly by US Congress shortly after the events of September 11, 2001, with a number of provisions that were scheduled to “sunset” in five years unless the US

Government could persuade Congress to make them permanent. They succeeded in doing so in March 2006, and the controversial clauses became permanent. This Office has certainly expressed concerns about our own Anti-terrorism Act in previous Annual Reports, and noted the growing concern about the impact of foreign legislation on personal data that has left Canada.

This issue has certainly caught the imagination of Canadians, and we have received inquiries and complaints which focus on it as a threat to the privacy of Canadians where transborder dataflow is an issue. It is perhaps appropriate to remind everyone that once data is outside of Canada, the ultimate control of it rests in the hands of the authorities in that state. It is subject to the Court systems in that country, and is accessible under local laws. This is why the European Union passed its Directive 95/46 on Privacy, which directs EU data protection commissioners to block dataflows to foreign states without “adequate” data protection. Adequate data protection includes not merely data protection law, but independent data protection authorities who can provide redress for the citizen.

This is old hat to those who follow data protection matters, because these provisions caused a tremendous stir in 1990s when the Directive was first introduced, but 15 years later we still only inching our way closer to finding solutions for disputes arising from global data flows. The Privacy Commissioner of Canada has agreed to sit on a committee of the Organisation for Economic Co-operation and Development (OECD) which is investigating the need for greater cooperation among independent authorities in handling cross border violation of data protection laws.

This Office has dealt with complaints about cross border marketing of information, and it is clear that dealing with jurisdictional issues is going to be a growing concern in data protection, just as it is in cybercrime. The Justice Minister in the last Parliament had indicated his support for ratifying the Council of Europe’s Cybercrime Treaty, which facilitates cooperation among signatories in fighting cross-border crime. We need privacy matters to be included in this agreement as well, or we need other administrative tools such as Mutual Legal Assistance Treaties and Memoranda of Understanding with other states.

We followed up the debates of 2004 on transborder data flow in early 2005. We wrote a letter to the President of the Treasury Board urging the federal government to review the implications of its outsourcing of personal information and to develop contractual clauses to protect personal information transferred to third parties for processing. In the following months we were consulted by the Treasury Board

Secretariat as it crafted a federal strategy in response to privacy concerns about the *USA PATRIOT Act* and the possibility that foreign legislation could reduce the protection of Canadians' personal information. The review of outsourcing contracts among 160 federal institutions revealed that more than 80% rated their contracts as having "no" or "low" risk. The review also helped departments and agencies identify measures to further mitigate privacy risks. One of the key documents released by the Treasury Board Secretariat was a set of guidelines for government institutions. The guidelines set out rules for outsourcing activities in which personal information about Canadians is handled or accessed by private sector agencies under contract with government institutions.

We see the federal strategy as a very positive step toward addressing Canadians' concerns about the flow of their personal information across borders and the possible privacy risks posed by foreign legislation, or even the absence of any privacy legislation. Personal data increasingly circulates the globe and is an important part of global commerce. International data protection rules, such as those of the OECD or the European Union, were created to facilitate the transfer of data across boundaries under appropriate conditions. The recent Treasury Board guidelines attempt to meet the same objectives and we hope that they will be an integral part of a reformed *Privacy Act*.

International Liaison

Over the past year, we have had several visits from colleagues in other countries, with a view to sharing our experiences in the field of data protection and assisting in the development of data protection law. In a world of global dataflows, it is increasingly important that despite differences in legal approach, we achieve harmonious results in our expectations of business practice. As we share data about our citizens, it will be important that we can count on the oversight of similar authorities outside our own jurisdiction, who will look after the protection of the privacy of Canadians.

In October-November we hosted a policy analyst from the *Commission nationale de l'informatique et des libertés* (CNIL), the data commission of France. We were honoured by a visit by the President of the CNIL, M. Alex Türk, and compared our different approaches to enforcement of law. In December we hosted two senior officers from the Mexican Federal Institute for Access to Public Information, who were interested in learning how our regime functions at the ground level, because Mexico is contemplating the enactment of data protection law, and indeed has a bill in Congress. Following their visit, we prepared for a much larger delegation who ultimately arrived for a three day visit in May 2006.

We look forward to hosting the International Conference of Data Protection and Privacy Commissioners in September 2007, where many world experts in privacy and data protection will gather in Montreal. This is a tremendous opportunity for Canadians in government, business, civil society and academe to gather and benefit from the assembled expertise. We will continue to work with colleagues to develop the individual exchange program, a highly useful and relatively inexpensive way to develop harmonized approaches, share knowledge, and build effective relationships.

Radio Frequency Identification Devices (RFIDs)

We have been analyzing the potential impact of Radio Frequency Identification Devices on personal privacy, and how our legislation would apply. The devices have potential for widespread use in consumer products in Canada. With respect to the public sector, there have been suggestions to put RFIDs in passports and border crossing cards. We put a fact sheet up on our web site, and are working on further guidance which will appear this coming year.

Video surveillance Guidelines

The Office has been working with the Royal Canadian Mounted Police (RCMP) to develop video surveillance guidelines for the use of cameras to monitor public spaces. We have put the guidelines on our web site, and continue to study both increasing use of cameras, and the technical advances that have helped make such surveillance so prevalent now, not only in public spaces, but in retail environments, the workplace, and near all kinds of facilities that have importance with respect to critical infrastructure protection, from gas pipelines to nuclear sites. The increasing power of these cameras, the decreasing costs of data storage, the development of good facial recognition and computer programs that do movement pattern recognition, coupled with the ease with which even remote cameras can now be linked to the world wide web have certainly created the potential of a powerful web of surveillance. We are witnessing an increasing appetite for video-surveillance in Canada and will be developing further guidance on the issue.

Identity Management and the War on Crime and Terror

One of the recurrent themes of this year's research and policy analysis has been identity management. This Office has written about this issue from many perspectives over the past twenty-three years, from discussions on the use of the Social Insurance Number to the OPC's submission on biometric identity cards. This year, we decided that identity management will be a focal point for next year's

research and policy agenda. Here are a few of the experiences of 2005-06 that have led us to this conclusion.

We have been immersed in issues surrounding border security, whether through the audit we conducted of the Canada Border Services Agency which is described later in this report, through commenting on speculation about the proposed Canada-US border card, or in our questions to Transport Canada on no-fly lists. While it is perfectly legitimate for sovereign states to want to positively identify who is crossing into their countries, we are concerned that once a card is introduced, it will be swiped or presented in a host of new situations. It is our observation that when we are frightened about potential terrorist and criminal activity, the impulse is to throw the lights on and identify everything, like a child frightened in the dark. It has not been made clear to us that uniquely identifying each person will enable us to predict who is good or bad, although it may indeed help to prevent fraud in some cases. Nevertheless, teasing apart the reasons for new cards, new identity schemes, new registers of people, and responding to the fresh losses of anonymous transactions in our daily lives is occupying a significant part of our time.

It seems obvious to observe, in relation to the no-fly list for instance, that surely if a person is too dangerous to be allowed to sit in an aircraft, they might be also too dangerous to sit on a subway or board a train. Where are we going with this kind of thinking? As we examine the application in other jurisdictions of RFID chips in motor vehicle licence plates, reporting on where and when vehicles are traveling on the streets and highways, is it not natural to inquire when we will see these devices on people? Someone has to ask these questions, perhaps it is our duty.

With respect to the questions we sent to Transport Canada on the no-fly list issue, the Commissioner stated publicly in August 2005 that this could be a “serious incursion into the rights of travellers in Canada, rights of privacy and rights of freedom of movement.” In May 2006 we received a privacy impact assessment for the project and it is currently under review.

At the routine, day to day level, the federal government is working to improve electronic service delivery. Service Canada is working to roll out integrated service delivery, responding to the needs of Canadians for something that feels like the one-stop shopping they now get at the supermarkets. The architecture behind these offerings will continue to challenge us as we try to ensure streamlined process without facilitating the development of a Panopticon in government, where the central authority can see everything.

Technology leaders such as Microsoft and IBM are presenting new schemes for identity management, to deal with issues of fraud, SPAM, and consumer usability, among others. Telecommunications companies, responding to our own concerns about providing personal information only to the person it concerns, are initiating newer and tougher authentication regimes. Banks are being asked by government to provide more data about individuals and their transactions. We have examined the Financial Crimes Reporting legislation, in anticipation of the review of the Act in 2006, and we are concerned about the degree of surveillance of financial transactions which this Act has mandated. Who among Canadians have any idea where their financial data is going, and what is happening with the information reported by banks, accountants, lawyers, and other private sector players about their customers? Even if the data is perfectly managed, and we had time to audit the relevant players to determine this, the point is that in this democracy there are very few who understand the extent of the growth of surveillance and data gathering, and that in itself is a worry.

Sometimes when we meet with our colleagues in government to discuss new initiatives, we ask questions that may seem a little offensive. Canada is not by any means an oppressive state, and officials in the federal government are absolutely impressive in their desire to maintain privacy protections, to understand the impacts of complex technological implementations, and in their respect for human rights and civil liberties. But the price of freedom is, indeed, eternal vigilance. Where will the thirst for identification and transactional surveillance lead us? Is it possible for us to manage all of this disparate activity and come up with an approach to identity and authentication that we could dare to call comprehensive?

We are certainly going to try. There has been a lot of work done in other jurisdictions. We are encouraged that the Treasury Board Secretariat is looking at some of these issues here in Canada, and we hope to play our part in contributing the privacy perspective to the dialogue. Indeed, identity is not that easy.

COMPLAINTS

Since 1983 this Office has investigated complaints dealing with personal information held by federal government departments and agencies. The *Privacy Act* governs the collection, use, disclosure, retention and disposal of personal information in the administration of government programs and provides individuals with the right of access to their government-held personal information. The Privacy Commissioner of Canada normally deals with complaints filed by individuals, but she may initiate a complaint and investigate a situation where she has reasonable grounds to believe the *Privacy Act* has been violated.

The Privacy Commissioner is an ombudsman who resolves complaints through mediation, negotiation, and persuasion whenever possible. However, the *Act* gives the Commissioner broad investigative powers to carry out her mandate. She may subpoena witnesses, compel testimony, and enter premises to obtain documents or to conduct interviews. The Commissioner can and does recommend necessary changes to the information-handling practices of government institutions.

Definitions of Complaint Types

Complaints received in the Office are categorized into three main groups:

Access:

- **Access** – All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.
- **Correction/Notation** – The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.

- **Language** – Personal information was not provided in the official language of choice.
- **Fee** – Fees have been assessed to respond to a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.
- **Index** – INFOSOURCE ¹ does not adequately describe the personal information holdings of an institution.

Privacy:

- **Collection** – Personal information collected is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.
- **Retention and Disposal** – Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in INFOSOURCE): either destroyed too soon or kept too long.
In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.
- **Use and Disclosure** – Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible disclosures without consent listed in section 8(2) of the *Act*.

Time Limits:

- **Time Limits** – The institution did not respond within the statutory limits.
- **Extension Notice** – The institution did not provide an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.
- **Correction/Notation - Time Limits** – The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

¹ INFOSOURCE is a federal government directory that describes each institution and the banks of information (groups of files on the same subject) held by that particular institution.

Complaints Received between April 1, 2005 and March 31, 2006

The Office received 1,028 complaints in 2005-06, 549 fewer complaints than the previous year. This 35% decline from the previous year reflected lower numbers of Access, Use and Disclosure and Time Limits complaints. As opposed to last year, the Office did not receive any groups of complaints, which may also account in part for the lower number of complaints received.

Complaint Type	Count	Percentage
Access	391	38.00
Collection	25	2.40
Correction-Notation	44	4.30
Correction/Notation - Time Limits	9	0.90
Extension Notice	22	2.10
Language	1	0.10
Retention and Disposal	10	1.00
Time Limits	411	40.00
Use and Disclosure	115	11.20
Total	1,028	100.00

As in previous years, the most common type of complaint concerned institutions not meeting the 30-day timeframe specified in the Act to respond to requests for access to personal information. Time limit complaints, along with complaints about denial of access to personal information and inappropriate use and disclosure of personal information, comprise 89% of the complaints received. In the 2004-05 fiscal year the distribution was similar, with these complaints constituting 85% of the total.

Top Ten Institutions by Complaints Received

The following table represents the institutions that received the greatest number of complaints in the fiscal year ending March 31, 2006.

Organization	Total	Access	Time Limits	Privacy
Correctional Service Canada	190	108	43	39
Royal Canadian Mounted Police	165	35	121	9
Immigration and Refugee Board *	121	32	85	4
Canada Revenue Agency	92	38	37	17
Citizenship and Immigration Canada	60	32	27	1
Canada Post Corporation	42	15	17	10
National Defence	41	13	21	7
Human Resources Skills Development	35	10	5	20
Canadian Security Intelligence Service	35	30	5	0
Canada Border Services Agency	34	12	19	3
Others	213	111	62	40
Total	1,028	436	442	150

* A significant portion of complaints regarding this institution were submitted by one individual in the course of dealing with the Immigration and Refugee Board.

The number of complaints filed against institutions does not necessarily mean that these institutions are not compliant with the *Privacy Act*. Because of their mandate, some of these institutions hold a substantial amount of personal information about individuals and are therefore more likely to receive numerous requests for access to that information. Holding a large amount of personal information increases the likelihood of complaints about the institution's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

Complaints Received by Institution

This table shows the actual number of all of the complaints lodged against the various institutions and agencies that were received in the fiscal year ending March 31, 2006.

	Total
Agriculture and Agri-Food Canada	32
Canada Border Services Agency	34
Canada Economic Development for Quebec Regions	13
Canada Firearms Centre	1
Canada Post Corporation	42
Canada Revenue Agency	92
Canadian Air Transport Security Authority	2
Canadian Food Inspection Agency	1
Canadian Heritage	1
Canadian Human Rights Commission	4
Canadian Security Intelligence Service	35
Citizenship and Immigration Canada	60
Commission for Public Complaints Against the RCMP	1
Correctional Investigator Canada	1
Correctional Service Canada	190
Elections Canada	1
Export Development Corporation	8
Fisheries and Oceans	1
Foreign Affairs and International Trade Canada	33
Health Canada	18
Human Resources and Skills Development Canada	35
Immigration and Refugee Board	121
Indian and Northern Affairs Canada	3
Indian Residential Schools Resolution Canada	1
Industry Canada	5
Justice Canada	29
Library and Archives Canada	7
National Defence	41
National Gallery of Canada	1
National Parole Board	4
National Research Council Canada	2
Office of the Commissioner of Review Tribunals	1
Pacific Pilotage Authority Canada	1
Pension Appeals Board Canada	2
Privy Council Office	1
Public Safety and Emergency Preparedness Canada	1
Public Service Commission Canada	7
Public Works and Government Services Canada	6
Royal Canadian Mounted Police	165
Social Development Canada	13
Statistics Canada	3
Transport Canada	3
Veterans Affairs Canada	6
Total	1,028

Complaints Received by Origin

From April 1, 2005 to March 31, 2006

The following table shows the province of origin of the complaints received in the reporting period. It should be noted that some complaints were received from persons living outside Canada. Canadians living outside the country whose personal information is held by the Canadian government are also covered by the *Privacy Act*.

Province/Territory	Total	Percentage
Quebec	249	24.00
Ontario	225	22.00
British Columbia	182	18.00
NCR	159	15.00
Alberta	68	7.00
Manitoba	53	5.00
Saskatchewan	35	3.00
International	17	2.00
New Brunswick	15	1.50
Nova Scotia	16	1.60
Newfoundland	5	0.50
Prince Edward Island	2	0.20
Yukon Territory	2	0.20
Total	1,028	100.00

Almost 80% of complaints originated in the provinces of Quebec, Ontario and British Columbia, as well as in the National Capital Region. This pattern is consistent with what we have seen over the last five years in that Quebec, Ontario, and British Columbia have, with one exception, been the source of the vast majority of complaints received. The exception was in the 2003-04 year, when Alberta bumped Ontario out of third place.

Complaints Completed between April 1, 2005 and March 31, 2006

In the past fiscal year, we closed 1,040 complaints, approximately the same number of complaints that we received in that year.

Despite closing as many *Privacy Act* complaints as received, the Office is carrying a significant number of ongoing cases – 1,263 at fiscal year-end. A major Business Process Review of the Branch was finalized at the beginning of the year to establish appropriate resource levels and to find solutions to our aging caseloads. A requirement for additional resource levels was identified and intensive staffing activities are underway to recruit, hire and train additional investigators. We are determined to deal with the backlog of cases within two years.

Definitions of Findings and other Dispositions under the *Privacy Act*

The Office has developed a series of definitions of findings to explain the outcome of its investigations under the *Privacy Act*.

Early resolution: applied to situations in which the issue is dealt with before a formal investigation is undertaken. For example, if an individual complains about an issue that the Office has already investigated and found to be compliant with the *Privacy Act*, we explain this to the individual. We also receive complaints in which a formal investigation could have adverse implications for the individual. We discuss the possible impact at length with the individual and should he or she choose not to proceed further, the file is closed as “early resolution”.

Not Well-founded: the investigation uncovered no or insufficient evidence to conclude that the government institution violated the complainant’s rights under the *Privacy Act*.

Well-founded: the government institution failed to respect the *Privacy Act* rights of an individual.

Well-founded/Resolved: the investigation substantiated the allegations and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: after a thorough investigation, the Office helped negotiate a solution that satisfies all parties. The finding is used for those complaints in which well-founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

Settled during the course of the investigation: the Office helped negotiate a solution that satisfies all parties during the investigation, but issues no finding.

Discontinued: the investigation was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons —the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Findings by Complaint Type

The following charts show the outcome of our investigations of the different types of complaints we receive. The first chart represents all types of complaints; the second represents access and privacy complaints, and the third represents complaints strictly related to time limits. This is the first time we have isolated our statistics in this way to demonstrate the significant number of complaints we receive that are related strictly to time limits.

Complaints (All Types) Closed

From April 1, 2005 to March 31, 2006

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Access	54	12	143	12	63	1	23	308
Collection	2	2	19	0	9	1	0	33
Correction-Notation	24	1	3	0	5	0	0	33
Correction/Notation - Time Limits	0	0	0	0	0	5	0	5
Extension Notice	2	1	37	0	0	4	0	44
Language	0	0	0	1	0	0	0	1
Retention and Disposal	0	0	2	0	4	1	0	7
Time Limits	47	5	22	11	8	395	0	488
Use and Disclosure	12	2	51	2	29	25	0	121
Total	141	23	277	26	118	432	23	1,040

Access and Privacy Complaints Closed

From April 1, 2005 to March 31, 2006

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well founded-Resolved	Total
Access	54	12	143	12	63	1	23	308
Collection	2	2	19	0	9	1	0	33
Correction-Notation	24	1	3	0	5	0	0	33
Language	0	0	0	1	0	0	0	1
Retention and Disposal	0	0	2	0	4	1	0	7
Use and Disclosure	12	2	51	2	29	25	0	121
Total	92	17	218	15	110	28	23	503

Clearly, there are far more not well-founded complaints than well-founded complaints: 218 and 51 respectively. This includes well-founded resolved. In addition, a significant number of complaints are resolved in some way (discontinued, early resolution, resolved or settled in the course of investigation): 234 out of 503 complaints, or 47%. Another way of viewing this is that only 10% of complaints to our Office under the *Privacy Act* are well-founded. We believe this speaks well for overall compliance with the Act by federal institutions.

Appendix 1 provides a detailed breakdown of access and privacy complaints closed by department.

Time Limit Complaints Closed

From April 1, 2005 to March 31, 2006

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Correction/Notation - Time Limits	0	0	0	0	0	5	0	5
Extension Notice	2	1	37	0	0	4	0	44
Time Limits	47	5	22	11	8	395	0	488
Total	49	6	59	11	8	404	0	537

It is important to note that of a total of 537 complaints, 75% of these were well-founded. By their very nature, the majority of Time Limit complaints are well-founded. Organizations have 30 days from the date of receipt to respond to requests from individuals for access to their personal information. Individuals do not complain unless there has been a delay in responding to their requests. The exceptions to well-founded findings are as a result of appropriately applied Extension Notices to allow for an additional 30 days to respond and instances where the complainants did not allow for mailing time; e.g. a request must be received by the institution before starting the 30-day count.

The OPC remains concerned, however, about the numbers of Time Limit complaints lodged against some institutions. The OPC is aware that some of these institutions have taken steps to address resourcing deficiencies. Experience shows that public service staffing takes considerable time, as does training of new staff. There is therefore some lead time between identifying a requirement for resources and having that translate into increased productivity and a decrease in backlogs. The OPC will continue to monitor and assess compliance with the Time Limit requirements of the *Privacy Act* in the coming year.

Appendix 1 provides a detailed breakdown of time limit complaints closed by department.

Complaint Investigations Treatment Times - *Privacy Act*

The following tables show the average number of months taken to complete a complaint investigation, from the date the complaint is received to when a finding is made. The first table breaks this down by finding, the second by complaint type.

By Finding

For the period between April 1, 2005 to March 31, 2006

Disposition	Average Treatment Time in Months
Early Resolution	3.61
Well-Founded	7.18
Not Well-Founded	13.22
Discontinued	8.96
Settled in the Course of Investigation	16.46
Well-Founded, Resolved	23.09
Resolved	14.27
Overall Average	10.49

By Complaint Type

For the period between April 1, 2005 to March 31, 2006

Complaint Type	Average Treatment Time in Months
Correction/Notation - Time Limits	9.20 *
Extension Notice	8.45
Time Limits	6.49
Access	15.14
Language	25.00 **
Use and Disclosure	14.25
Collection	14.64
Retention and Disposal	23.86
Correction/Notation	9.73
Overall Average	10.50

* The treatment time for this complaint type is based on five cases.

** The treatment time for this complaint type is based on one case only.

The treatment times reflected above are of concern since our average time elapsed from the date of complaint to the date of finding is ten and a half months. The breakdown by finding shows that complaints that require full investigation – that is,

the complaints that result in findings of well-founded/resolved, resolved, not well-founded or settled – take on average more than a year to complete. The delay in completing settled complaints reflects the long standing practice of this Office not to settle cases until the investigation has been finalized. However, we are pleased to report that we have changed this practice and now a case can be settled at any point during the investigation, which should reduce treatment times for settled cases.

Follow-up after Investigations

Once a complaint is investigated and completed, the story does not necessarily end there. All complaints dealing with improper collection, use, disclosure and retention that are well-founded are sent to the Audit and Review Branch for its review. This allows the Branch to identify any trends and patterns dealing with privacy breaches and use this information in planning and developing its audits for the next year.

Select Cases under the *Privacy Act*

The following summaries provide a sample of the types of complaints received and the approach taken by this Office to address various issues with regard to personal information protection in the public sector. These cases demonstrate how important it is for government institutions and agencies to be ever vigilant in handling personal information and what can go wrong when this does not occur.

Subscribers required to provide information to renew e-mail news subscription

A subscriber to an e-mail media news service complained that he had to provide more information than was necessary in order to re-subscribe. It was the Department of Foreign Affairs and International Trade (DFAIT) that offered the subscription service. Specifically, the complainant objected to providing his postal code, telephone number and company affiliation. He also was upset that although DFAIT's privacy notice said the provision of information was voluntary, it was actually obligatory.

The Office learned that DFAIT had been asking Canadian subscribers to its e-mail media releases to provide their e-mail address, city, province, postal code, telephone number and company affiliation. International subscribers were only being asked for their e-mail address and country of origin. We confirmed that the on-line subscription application would not accept the subscription without this information.

DFAIT explained that telephone numbers are required so that the department can contact subscribers in the event of any technical problems with e-mail addresses. Postal code and company affiliation information is required so that some media releases can be targeted to a particular region or a particular type of business.

Our Office concluded that DFAIT was allowed under the Act to collect the subscriber information in order to facilitate access to and distribution of the media releases. The complaint was therefore considered to be not well-founded. However, we were pleased that DFAIT agreed that the use of the word “voluntary” in its privacy notice was somewhat misleading; it was, in fact, the participation in the subscription activity itself that was voluntary. DFAIT subsequently changed the notice to make it more accurate.

Unnecessary requirement for a social insurance number

A caregiver complained that she had to give her social insurance number (SIN) to the father of a child in her care. It was required in order for the father to receive compensation under the Department of National Defence's (DND) Family Care Assistance (FCA) program.

Under DND's FCA program, certain members of the Canadian Forces can be reimbursed for child care costs when on duty away from home. In order to receive the benefit, members have to submit receipts and complete a DND form, which requests information concerning the caregiver, including the caregiver's name, SIN or business number.

During our investigation, DND explained that there was no actual requirement for the caregiver's SIN under the FCA program. It therefore agreed to change its form to reflect this. In the meantime, DND instructed its staff not to ask for the SIN. DND also confirmed that the father in question had not provided the caregiver's SIN on the form.

The caregiver was pleased with this outcome, and the matter was considered settled.

Human rights complaint investigation prompts release of employee information

An employee of the Canada Post Corporation (CPC) complained that the CPC had told another organization that she had taken disability leave from her job.

Our Office learned that the CPC employee had initiated a human rights complaint against her employer on the issue of duty to accommodate based on a medical disability. During the CPC's investigation into the circumstances that led to the human rights complaint, a concern emerged as to whether the employee had held another job while on disability leave from the CPC.

In accordance with the basic principles of procedural fairness in the conduct of any investigation, an investigator is obligated to explain the nature and scope of the matter under investigation in order to elicit accurate and relevant information.

In order to check the facts, the CPC contacted the other organization to inquire about the individual's employment. The CPC informed the organization that it was investigating a human rights complaint filed against it based on a medical disability and the type of information it was seeking. Before releasing any of the complainant's information to the CPC, the other organization requested her consent and referred to her having taken disability leave. However, we determined that this statement was an assumption on the organization's part as there was no evidence that anything was said by the CPC about the complainant being on disability leave.

As this individual's information, which the CPC gave to the organization, was necessary and directly related to the conduct of the human rights investigation, our Office concluded that the complainant's privacy rights were not affected and this matter was not well-founded.

Collection officer did not divulge debtor personal information

An individual complained that a Canada Revenue Agency (CRA) collection officer improperly disclosed her personal information to another person.

Our Office learned that the complainant owed the CRA for overpayment of the Canada Child Tax Benefit (CCTB). She had been entitled to the benefit while she was married. However, she continued to receive the benefit following her divorce, even though she had not been awarded custody of her children. The CRA discovered the overpayment when her ex-husband and mother-in-law, who was the children's

caregiver, applied for the benefit. The CRA was able to recover a portion of the overpayment but, after a while, its letters requesting payment of the remainder of the debt were returned unopened.

A CRA collection officer then reviewed the file, and phoned the mother-in-law, whose name was on record as the current recipient of the CCTB. Our Office was informed by the collection officer that she identified herself to the mother-in-law and stated that she was trying to track down the daughter-in-law's current contact information. The complainant maintained that the collection officer then divulged her personal tax information concerning the CCTB. However, both the CRA officer and the mother-in-law denied this. Both maintained that the mother-in-law immediately guessed why the officer was trying to contact the daughter-in-law, and, upon being questioned, the officer said she could not disclose any details.

Under the *Income Tax Act*, CRA collection officers have been delegated responsibility for collecting tax debts owed to the Government of Canada. In this instance, the evidence indicated that the CRA's collection officer did not provide any details regarding the complainant or her tax file to the complainant's mother-in-law. In our view, the Collections Officer followed the basic principles of an investigator's obligations of procedural fairness. The person merely introduced herself as a CRA Collections Officer and requested contact information for the complainant. Our Office therefore considered the complaint not well-founded.

PSC discloses information in an audit

Three individuals complained that the Public Service Commission (PSC) disclosed information about them in an audit that it had conducted and released to the public.

The PSC audited the staffing actions of a small government organization. In its report of findings, it cited examples of specific staffing actions that it had examined. Our Office found that, while the report did not contain any names, it provided enough detail about some specific cases that the individuals could be identified. Furthermore, as the audit was made public, its findings were reported in the media.

Audits are generally negative in nature, and it is not unusual that they should contain examples of scenarios portrayed in negative terms. This is not problematic when speaking of staffing processes for federal institutions with hundreds of employees in particular job classifications. However, when it is a small institution,

it is a different matter. Furthermore, calling into question the selection process of a position when the individual is identifiable directly reflects on the person's competence and qualifications.

Our Office concluded that the information released by the PSC in its audit was clearly the individuals' personal information and should not have been disclosed without each person's consent. The complaints were therefore well-founded.

Our Office is pleased to report that the PSC now requires all of its audits to be reviewed by its Access to Information and Privacy Branch before they can be released to determine if they contain information which is subject to the *Privacy Act*.

Government has right to monitor use of its e-mail systems

A Canada Border Services Agency (CBSA) employee was annoyed that each time he logged on to his CBSA computer system, he had to agree to an online statement or else be denied access to the system. The statement in question indicates that the CBSA may monitor the use of its systems. The complainant maintained that the use of e-mail should receive the same privacy considerations as use of the telephone. In his view, monitoring his e-mails violated his privacy rights.

Our Office ascertained that the CBSA's monitoring policy is drawn from two Treasury Board policies: the Government Security Policy and the Policy on the Use of Electronic Networks. These policies clearly state that government departments must conduct active monitoring and internal audits of their security programs. As such, electronic networks may be monitored for operational reasons and for assessing compliance with the policies. While normal routine analysis does not involve reading content, if due to routine analysis or a complaint the institution reasonably suspects that an individual is misusing the network, the matter is referred for investigation and action that may involve special monitoring and/or reading the content of the e-mails. In this case, the CBSA confirmed that the complainant's personal e-mails were never read.

The CBSA pointed out that e-mail is a corporate communications tool provided to employees for the purpose of conducting official government business. The department allows limited personal use when it complies with CBSA's policies and legislation, and when employee performance is not adversely affected.

Our Office concluded that the CBSA displayed fairness and transparency by informing its employees of its monitoring practices through the online statement, and by making the electronic network policy guidelines readily available on its intranet. Employees therefore have clear expectations of the level of privacy they can expect from the employer. Our Office determined that the complaint was not well-founded.

Incidents under the *Privacy Act*

In addition to individual complaints, our Office investigates incidents of mismanagement of personal information. These are typically brought to our attention from various sources including the media and directly from institutions themselves, and may involve matters of improper collection, use or disclosure of personal information. They often highlight a systemic issue, or an unrecognized privacy breach that needs to be corrected as soon as possible. Last year, the Office completed 54 such investigations.

There were a number of incidents involving computer theft or briefcase theft, three incidents involved information on shared computer drives and two incidents involved the sale of fax machines that retained personal information in a memory component. These cases are described below.

Thermofax rolls containing personal information sold by Crown assets

There have been a couple of incidents in which fax machines purchased at Crown Assets Distribution Centre sales were found to hold rolls that still contained personal information. For example, in 2005, Human Resources and Skills Development Canada (HRSDC) reported to our Office that a member of the media had obtained a thermofax roll containing the names and/or Social Insurance Numbers of 65 individuals. A thermofax roll comes in a cartridge that is loaded into the fax machine. It contains a combination of a thin sheet of paper and a clear film-like substance. When the paper on the cartridge has all been used and the cartridge needs to be replaced, the used film has the negative image of every single fax that came through that machine from the time the roll was installed until it was removed. The thermofax roll had been sold as part of a fax machine at a Crown Assets sale and was later acquired by an individual who passed the roll on to the media. Following HRSDC's investigation, the purchaser assured officials that he had destroyed the thermofax roll and all records that had been retrieved from it.

HRSDC took several steps to ensure that this type of situation does not recur. An amended policy was circulated to HRSDC, Social Development Canada and Service Canada that reinforced the need for the inspection of business equipment being declared surplus and the need for the removal and suitable destruction of ‘memory instruments’. Officials agreed to undertake a complete physical inventory and reconciliation of all fax machines. They also contacted Crown Assets to retrieve any unsold equipment of this type to check it for personal information. Our Office was satisfied that all appropriate action had been taken to remedy the situation and to prevent future occurrences.

However, during our investigation, we discovered that two fax machines with thermofax rolls intact and originating from the Canada Revenue Agency (CRA) had also been sold by Crown Assets. Again, the staff was simply unaware of the need to sanitize such equipment. CRA too has amended its policies and procedures with respect to disposal of equipment with memory capability.

Given the far-reaching implications of this matter and the likelihood that every department and agency is using some type of equipment with memory that requires special disposal, our Office advised the Information, Privacy and Security Policy Directorate at the Treasury Board Secretariat. It too is pursuing the matter and will be issuing a bulletin to all government departments and agencies.

In conclusion, this highlights the importance of all institutions ensuring that personal information is properly erased from electronic data storage devices. The subject is not straightforward but there are three ways for “media sanitization” or destruction of electronic data:

- **Overwriting** – overwriting with 1s and 0s where the data was located
- **Degaussing** – magnetically erasing the data with an electric degausser
- **Destruction** – physical destruction of the storage medium

Two technical documents provide advice on these topics:

- Communications Security Establishment *Clearing and Declassifying Electronic Data Storage Devices*, available online at <http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg06.pdf>
- U.S. Department of Defense Standard 5220.22-M – Advising Users on Computer Systems Technology, available online at http://www.qsg.com/usdod_standard_dod_522022m.htm

Although these documents do not provide specific guidance on the destruction of thermofax rolls, the general techniques outlined in the documents (e.g. shredding) should be readily adaptable.

Laptop with NCC festival security-pass information stolen

An incident concerning computer theft occurred in the spring of 2004, involving a laptop computer and related accessories stolen from a National Capital Commission (NCC) facility. The laptop contained personal information consisting of two security databanks for security passes to various NCC festivals. The information, including names, photos, dates of birth, occupations and names of employers, was protected by two levels of passwords.

The NCC's internal investigation revealed that there had been major construction work going on in the building in question when the laptop was stolen. More people than normal had access to the premises where the computer was located, and it was very difficult to ascertain who might have taken it. The NCC undertook to increase the level of security in its facility. Our Office confirmed that the NCC also sent out letters to the employees whose information was compromised, referring them to a number of websites, including ours, for information on how to protect themselves from identity theft. They were also referred to the NCC's Access to Information and Privacy Office for further advice. In addition, our Office recommended to the NCC that it make an archive copy of this particular Information Bank in order to prevent any future loss in cases of theft or destruction of equipment.

Briefcase and knapsack containing offender information stolen from trunk of car

During the winter of 2005, two Correctional Service Canada (CSC) employees put a locked briefcase and a knapsack in the trunk of their personal car after leaving a meeting. Upon arriving home, they did not remove the items from the trunk. Two days later, one of the employees parked the vehicle at a mall, and upon return, discovered that it had been broken into. The next day, both employees checked the trunk and found that the briefcase and knapsack were missing. They immediately notified the RCMP and their employer. The RCMP did not conduct an investigation as CSC was to conduct its own.

Among the missing documentation was a report that contained information about eight federal offenders. CSC advised only two of the offenders about this incident, as the others were deceased. CSC's review concluded that it was not appropriate to transport protected information in a knapsack, and that neither the car trunk nor

the briefcase is an approved storage container for protected information. A briefcase, however, can be used to transport such information. In addition, the employees responsible for the protection of the information should have removed it from the vehicle when they reached their destination. As a result of this incident, CSC decided to establish more specific guidelines to provide direction concerning the transportation and storage of information outside of CSC premises.

DND employee finds own grievance information on shared computer drive

There have been a number of incidents regarding shared computer drives that resulted in personal information being accessible to people with no right to see it. In one instance a DND employee discovered a grievance chart on a shared drive. On the grievance chart was his name, the file number assigned to his grievance complaint and the status of his grievance. Similar information appeared on the list about other grievors as well.

During its investigation into the matter, DND learned that the information was originally on a protected drive with access shared on a controlled basis, limited to people who needed the information in order to do their jobs. At one point, servers were migrated, thus removing the firewall protection and making the information available on a shared drive for a limited time. This resulted in the employee being able to find the list.

Once DND was notified of the problem, it took immediate steps to remove and destroy the list. The grievance list has since been modified so that it no longer contains the identity of the grievors. DND reminded the group responsible for the list of the need to protect personal information. It also wrote to the employee, informing him of the situation that led to his information becoming available on the shared network. DND also advised him of his right to file a formal complaint with our Office.

Public Interest Disclosures under the *Privacy Act*

Heads of government institutions have the discretion to disclose personal information without an individual's consent when the disclosure benefits that individual or when a compelling public interest outweighs the invasion of the individual's privacy. The head of the institution is required to notify the Privacy Commissioner of such disclosures, in advance, unless the some urgency dictates otherwise. The Office reviews the proposed disclosures and, if deemed necessary, the Privacy Commissioner notifies the individual to whom the information relates. The Office also advises institutions when it believes the amount of personal information proposed for release is more than is needed to address the public interest and thus, we recommend measures to minimize the intrusion into the individual's life. Issues surrounding this provision in the *Privacy Act* are discussed earlier in this report.

We completed reviews of 66 such notices, a large number of them in two categories. The first category concerns individuals who were either unlawfully at large or being released from custody at the end of their sentences. All were considered at high risk to re-offend and therefore a danger to the community. We received 17 notices of this type, the majority of which came from the Royal Canadian Mounted Police and the Correctional Service Canada (CSC).

The second significant group – 13 – came from the CSC, National Defence and the National Parole Board. They concerned the disclosure of personal information to family members of recently deceased individuals to provide them with the circumstances of death and with some modicum of closure.

Another seven notices dealt with government accountability on matters such as the Ipperwash Inquiry with respect to the shooting of Dudley George, and the Board of Inquiry into the fire on HMCS Chicoutimi.

Also of interest were six notices concerning health issues, including one from Public Safety and Emergency Preparedness Canada and one from the Department of Foreign Affairs and International Trade Canada (DFAIT) on health risks to the public from individuals with tuberculosis.

There were also a variety of other notices, including one from the CSC regarding Karla Homolka, which provided information to her victims' lawyer about her release.

Investigation Process under the *Privacy Act*

Inquiry:

Individual contacts OPC by letter, by telephone, or in person to complain of violation of the Act. Individuals who make contact in person or by telephone must subsequently submit their allegations in writing.



Initial analysis:

Inquiries staff review the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act.

An individual may complain about any matter specified in section 29 of the *Privacy Act* – for example, denial of access, or unacceptable delay in providing access to his or her personal information held by an institution; improper collection, use or disclosure of personal information; or inaccuracies in personal information used or disclosed by an institution.



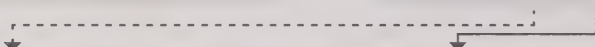
Complaint?

No:

The individual is advised, for example, that the matter is not in our jurisdiction.

Yes:

An investigator is assigned to the case.



Early resolution?

A complaint may be resolved before an investigation is undertaken if, for example, the issue has already been fully dealt with in another complaint and the institution has ceased the practice or the practice does not contravene the Act.

Investigation:

The investigation provides the factual basis for the Commissioner to determine whether the individual's rights under the *Privacy Act* have been contravened.

The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner or her delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

Discontinued?

A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.

Analysis (on next page)

Settled? (on next page)

Note: a broken line (---) indicates a *possible* outcome.

Analysis:

The investigator analyzes the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Branches, as appropriate.

Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the institution are warranted.

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the institution. The Privacy Commissioner or her delegate may ask the institution to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.

The possible findings are:

Not Well-Founded: The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the *Act* have been contravened.

Well-Founded: The institution failed to respect a provision of the *Act*.

Well-Founded, Resolved: The investigation substantiated the allegations and the institution has agreed to take corrective measures to rectify the problem.

Resolved: The evidence gathered in the investigation supports the allegations raised in the complaint, but the institution agreed to take corrective measures to rectify the problem, to the satisfaction of this Office. The finding is used for those complaints in which Well-Founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court on matters of denial of access to personal information.

Settled?

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through negotiation and persuasion. The investigator assists in this process.

Where recommendations have been made to an institution, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the denial of access. The Federal Court has the power to review the matter and determine whether the institution must provide the information to the requester.

Note: a broken line (----) indicates a *possible* outcome.

Inquiries

The Inquiries Unit responds to requests for information from the public about the application of the *Privacy Act* and *PIPEDA*. The Office receives thousands of inquiries each year from the public and organizations seeking advice on private sector privacy issues.

In the 2005-06 fiscal year, the Office received 2,506 inquiries relating to the *Privacy Act*. This is somewhat less than the number of inquiries in the previous year, when we received 2,976 inquiries. In comparison, we received more than double the number of inquiries on issues relating to *PIPEDA* (see statistics in our 2005 Annual Report to Parliament on *PIPEDA*).

The inquiries staff may be responding to fewer calls, but they are providing more information. A decision in 2004 to no longer accept e-mail inquiries has led to a refocusing of staff time on telephone inquiries, during which callers tend to seek longer and more in-depth explanations in response to their questions. In addition to this, an automated telephone system answers the public's most frequently asked questions, such as those about identity theft, telemarketing and the Social Insurance Number. Our web site also provides a wide range of information.

Approximately 25% of *Privacy Act* inquiries are answered in writing and 75% are answered by telephone. On average, written inquiries received a response within three months. The majority of telephone inquiries received an immediate response. The remainder, which may have required some research, received a response within three days.

Inquiries Statistics

April 1, 2005 to March 31, 2006

Privacy Act Inquiries Received by the Inquiries Unit

Telephone inquiries	1,929
Written inquiries (letter, e-mail, fax)	577
Total number of inquiries received	2,506

Privacy Act Inquiries Closed by the Inquiries Unit

Telephone inquiries	1,933
Written inquiries (letter, e-mail, fax)	631
Total number of inquiries closed	2,564

AUDIT AND REVIEW

The OPC is responsible for carrying out audits of federal departments and agencies subject to the *Privacy Act*. It may also carry out audits of private sector organizations pursuant to section 18(1) of Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)*. The OPC also evaluates Privacy Impact Assessments (PIAs) prepared by federal departments and agencies. It also undertakes a variety of other projects relating to privacy practices in both the public and private sectors.

The audit and review function of the Office serves its role as privacy guardian. The objective of this function is to conduct independent and objective audits and reviews of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability.

During fiscal year 2005-06, the Office completed one major audit pursuant to the *Privacy Act*, substantially completed three other audit projects and initiated a review of federal entities not subject to either the *Privacy Act* or *PIPEDA*. It also completed 43 PIA reviews, as well as 16 other projects. Staff also monitored the privacy-related activities of the Treasury Board Secretariat (TBS) and other federal departments and agencies.

Stronger Privacy Management Framework Needed to Ensure Sound Privacy Management

Last year the Office reported on the need for building a privacy management framework for the federal government. We outlined what a framework was, why it was important and described the features of a good privacy framework. We

also commented on some specific issues that needed to be addressed as part of strengthening privacy management in the federal government.

The Treasury Board of Canada Secretariat (TBS) is responsible for setting privacy policy direction and providing guidance to federal institutions. Last year the OPC recommended that TBS develop a model framework to guide privacy management in federal departments and agencies. TBS management accepted this, indicating that it was committed to the concept and that it would examine the scope and process for a project.

While the OPC is pleased to note good progress being made, all parties recognize there is considerable work yet to be completed.

In December 2005, TBS informed us that officials have begun to examine preliminary concepts for the design and development of a privacy management framework to set out the government's privacy vision and strategy. The framework will provide the foundation for a comprehensive privacy risk management and accountability infrastructure to ensure the right balance between the privacy rights of Canadians and the requirements to fulfill other public interest goals and program mandates. An initiative was underway to consolidate and update various privacy policies relating to privacy impact assessments, data matching, data protection and use of the SIN – all areas of concern to the OPC.

The OPC was consulted by TBS in developing a federal strategy to address concerns about the *USA PATRIOT Act* and Transborder Data Flows, mentioned earlier in this report. The government has responded well to the issue. In late March 2006, TBS published its strategy and issued guidance to federal government institutions for taking privacy into account before making contracting decisions. These documents are available on the TBS web site at www.tbs-sct.gc.ca. Among the activities reported as completed are the following:

- The government made all of its 160 institutions subject to the federal *Privacy Act* aware of the privacy issues raised by the *USA PATRIOT Act*.
- Institutions were asked to review their contracting and outsourcing arrangements to identify any risks under the *USA PATRIOT Act*, assess the seriousness of those risks, take corrective actions as needed, and report to TBS. It is reported that 83% classified their contracting as either “no risk” (77 institutions) or “low risk” (57 institutions).

- Best practices are promoted in outsourcing arrangements and a policy guidance document is available to federal institutions. It includes a privacy checklist, upfront advice on the importance of considering privacy prior to initiating contracts, ways of maximizing privacy protection and help in the development of clauses that can be included in requests for proposals and contracts.

The federal strategy also indicates additional steps to further mitigate risk to privacy. Some are listed below, and they illustrate the considerable amount of work required in fully dealing with the issue.

- Development of a privacy management framework to establish high standards for privacy protection throughout the federal government
- Follow-up assessment of federal contracting activities and ongoing contract advice from TBS
- Exploring technology and data architecture solutions to protect information flows, including the use of encryption technology and electronic audit trails
- Development of additional guidelines to cover government-to-government information sharing (within Canada and abroad), auditing of contracts, and technical solutions to protect privacy
- Increased awareness and training related to transborder data flows and existing federal safeguards
- A scheduled 2006 review of *PIPEDA* and the determination of whether the federal *Privacy Act* should also be reviewed (something the OPC strongly believes is long overdue)
- Addressing privacy and transborder data flows for the recently announced Security and Prosperity Partnership (SPP) between Canada, Mexico and the U.S.
- Sharing of best practices in protecting transborder data flows with provincial and territorial governments, as well as the private sector and foreign governments

We also applaud recent efforts by TBS to develop a privacy protection checklist – a set of principles and questions to guide government institutions in developing appropriate access to information and privacy clauses in contracts.

When contracting out, the management of a government program or service must ensure the contract does not weaken the right of public access to information or significantly impact on their department's ability to protect personal information

of individuals. This responsibility does not change when departments contract out services. An effective means to require that an outside service provider respects the requirements of the *Privacy Act* is to insert, when appropriate, relevant clauses in the contractual agreement. In this way, the contract helps ensure that the government institution's responsibility for the protection of personal information continues to be fulfilled by the contractor.

In March 2006 the OPC suggested that TBS pursue further enhancements to government contracting processes by considering the introduction of ways and means for businesses to report on their privacy management capabilities when seeking to become eligible to contract with the federal government. We see opportunity for further inculcating privacy management principles by incorporating privacy self assessment requirements into contracting arrangements with the federal government. This offers a powerful incentive to encourage businesses to comply with data protection principles as part of the social responsibility for doing business with the federal government.

The significance of transborder data flow is underscored by our audit of the Canada Border Services Agency, also discussed in this chapter. This reminds us that protection of personal information is integral to the operations of departments and agencies, and is not just a matter for contracting out to third parties. The OPC urges better management, as well as greater accountability to Parliament and the Canadian public.

The work of TBS on transborder data flow has advanced the building of a Privacy Management Framework. TBS indicates that such a framework would include best practices, sound risk management approaches and tools. The objective would be to ensure that federal institutions meet sound privacy management standards. We understand that TBS will establish an interdepartmental Privacy Committee that will collaborate on the continued development of the Privacy Management Framework.

We will continue monitoring developments and will examine how departments and agencies are adapting new contracting guidance when carrying out audits of federal entities subject to the *Privacy Act*.

Better Control and Accountability Required for Transborder Data Flow

A major audit of the Canada Border Services Agency (CBSA) has now been completed. The following is a summary of the audit results. The full report can be found on the OPC's web site at www.privcom.gc.ca.

Our audit of the CBSA and the review of public information about transborder data flow generally leads us to conclude that better control and accountability is required overall. Greater transparency should be given by government in order to allay public concern.

The audit of the CBSA is important since Canadians are concerned about the flow of their personal information to the United States and about the possibility that it may be used for reasons unrelated to anti-terrorism or trans-national crime prevention objectives. The public, as well as Parliament, want to know whether the CBSA, which is the federal government agency most directly involved in maintaining border security, is sharing personal information with its foreign law enforcement and intelligence partners in a way that complies with privacy legislation and that protects the privacy rights of Canadians.

Sound privacy management and accountability are essential in dealing with public concerns about the flow of personal information from Canada to other countries. Accordingly, the objective of the audit was to assess the extent to which the CBSA is adequately controlling and protecting Canadians' personal information as it flows to foreign governments. The audit focused on specific CBSA program areas and systems associated with the its management of personal information relating to travellers. Lines of examination included:

1. Customs enforcement and intelligence activities (land border and airports);
2. Integrated Customs Enforcement System (ICES);
3. Passenger Information System (PAXIS); and
4. National Risk Assessment Centre (NRAC).

The OPC also looked at the CBSA's overall framework for managing privacy and how it reports publicly on its sharing of personal information with other countries.

The approach and methodology included interviewing CBSA staff, examining documents (including records of trans-border sharing of personal information) and reviewing treaties, agreements, policies and practices which provide the framework for sharing this information between governments or their agencies. A special external advisory committee for the audit was formed to guide the work.

The audit reports findings are effective as of November 2005, the date when the examination was substantially completed.

Our Key Findings

The OPC found that the CBSA has policies, procedures and systems in place for managing and sharing personal information with other countries. However, much can be done to better manage the Agency's privacy risks and achieve greater accountability and control over personal information that flows across Canada's borders. Key findings are as follows.

- While written requests for assistance from foreign governments seeking CBSA documents are processed in accordance with Agency requirements, much of the information shared between the CBSA and the United States at the regional level is verbal, and not based on written requests. This contravenes CBSA policy and the Canada-United States *Customs Mutual Assistance Agreement* (CMAA) of June 1984.
- The CBSA needs a coordinated method of identifying and tracking all flows of its transborder data. The Agency cannot, with a reasonable degree of certainty, report either on the extent to which it shares personal information with the United States, or how much and how often it shares this information. By extension, it cannot be certain that all information-sharing activities are appropriately managed and that they comply with section 107 of the *Customs Act* and section 8 of the *Privacy Act*.
- Generally, the IT and management controls are sound for the Integrated Customs Enforcement System (ICES) and Passenger Information System (PAXIS). These systems contain sensitive personal information about millions of travellers. Notably, foreign jurisdictions did not have direct access to these systems. Secondly, electronic releases of information to the United States under the High Risk Travellers and Shared Lookout Initiatives of the CBSA are transmitted over secure communications channels. However, opportunities exist to strengthen the controls to further reduce the risk that personal information could be improperly used or disclosed.
- The CBSA needs to explore ways to improve the quality and control of data it acquires under the Advance Passenger Information/Personal Name Record (API/PNR) initiative to ensure that personal information used for fulfilling the Agency's customs mandate is as accurate and complete as possible.
- The CBSA has not yet evaluated the effectiveness of the High Risk Travellers (HRTI) initiative with the United States because this project has not yet

been fully implemented. In particular, the Agency should assess the extent to which inaccurate or incomplete data may affect individuals or the Agency's ability to identify, deter or apprehend "high-risk" travellers. An evaluation would help the Agency demonstrate that the HRTI initiative has achieved its enforcement and intelligence objectives and, accordingly, that its collection, use and sharing of vast amounts of personal information about millions of travellers are justified.

- Since the CBSA is a new agency, the time is ripe for the Agency to build and integrate a comprehensive privacy-management framework into its day-to-day information handling practices. In particular, the Agency should work toward updating and strengthening the obligations contained in its personal information sharing agreements with the United States. The Agency should also consolidate its reporting of privacy incidents and look for ways to improve its mechanisms for monitoring cross-border disclosures of personal information to foreign law-enforcement agencies and other institutions.
- Finally, the activities associated with sharing data across borders should be as transparent as possible. A clear and complete picture is not readily available with respect to what information is shared with whom, and for what purpose. As is the case for departments generally, the CBSA does not provide enough detail on the transborder flows of personal information, or account in a meaningful way for these flows to Parliament and the Canadian public.

Our audit resulted in 19 recommendations to the CBSA, which are available in our full report. Within two years the OPC will follow up to assess the progress the Agency has made in implementing the recommendations.

Importance of Privacy Impact Assessments

The Office reviews the Privacy Impact Assessments (PIAs) and Preliminary Privacy Impact Assessments (PPIAs) prepared by government institutions for various projects, and we make recommendations on ways to reduce the privacy risks to Canadians' personal information.

Privacy Impact Assessment is a tool that helps ensure that privacy protection is a core consideration when a project is planned and as it is being implemented. PIAs are meant to describe and document what personal information is collected, how it is collected, used, transmitted and stored, how and why it can be shared, and

how it is protected from inappropriate disclosure at each step. In short, it is a risk mitigation tool.

According to policy of the Treasury Board of Canada Secretariat (TBS), PIAs must be included in proposals for all new programs and services that raise privacy issues, and when existing programs are redesigned in a way that affects the collection, use or disclosure of personal information. This includes the conversion of government services for on-line use and delivery.

The TBS policy, which came into effect in 2002, also requires federal government institutions to submit their PIAs and PPIAs to our Office for review. This allows the OPC to analyze the data flow and the steps taken to address potential privacy concerns. We check to make sure an authority is in place that allows the collection and use of Canadians' personal information, and that the regulations and principles of the *Privacy Act* are being respected. We make comments to departments and agencies to identify potential problems that may have been overlooked and, as appropriate, we make recommendations for improving privacy protections. In some cases, we request that projects be considerably modified.

The OPC believes the PIA policy has had a great impact on improving the overall awareness of privacy within government institutions. In our view, it has focused attention on potential privacy issues of a number of government programs. The whole process provides a greater level of protection for the personal information that Canadians give to the federal government. A well functioning PIA practice is key for a sound Privacy Management Framework.

We are pleased to note that many of the PIAs we receive are becoming more precise and thorough in the years since the policy was first introduced. However, there is still considerable room for improvement. For example, the OPC has been encouraging departments to include in their submissions the action plans for implementing privacy protection strategies.

This fiscal year the OPC looked at a wide range of projects undertaken by a number of departments, including Human Resources and Skills Development Canada (HRSDC), Health Canada, the Royal Canadian Mounted Police (RCMP), Transport Canada, Indian and Northern Affairs Canada, Citizenship and Immigration Canada, Revenue Canada, the Canada School of the Public Service, Social Development Canada, Veterans Affairs Canada, Public Works and Government Services Canada (PWGSC), Statistics Canada, the Canadian Air Transport Security Authority, the

Canada Border Services Agency (CBSA), National Defence, Farm Credit Canada and the Canada Firearms Centre. As varied as the responsibilities of these departments are, the projects share a common characteristic – they all collect, retain, share or disclose the personal information of Canadians.

The following examples of PIAs offer an indication of the range and depth of the various projects we reviewed:

- The RCMP Integrated Query Tool, a web application that brings together information from several discrete police information data bases into a central repository to allow a single search capability and a consolidated report on an individual
- The RCMP Canadian Police Information Centre (CPIC) Renewal project and its sharing agreements with other jurisdictions
- A system which allows Employment Insurance (EI) claimants to complete and submit their required reports online, using computers at home or in employment centres
- A PWGSC project to contract foreign banking services in order for Canadians living overseas to receive government payments, such as pensions, in a timely fashion
- A Children's Respiratory Health Study, surveying 25,000 elementary school children
- A High Risk Traveller Identification Project in which the CBSA collects and shares with the United States information on individuals travelling by air to that country, and collects and analyses information on individuals arriving by air to Canada
- A pre-boarding screening project involving remote video surveillance of passengers in airport boarding areas across the country by the Canada Air Transport Security Authority (CATSA)
- An electronic health record project for the Canadian Armed Forces with the potential to contain the medical, dental and psychological health information for more than 80,000 Armed Forces personnel

- Citizenship & Immigration Canada's use of biometrics (fingerprints and photos) in field trials at border crossings and as a method of cross-checking refugee claimants

As illustrated above, the projects reviewed are diverse and in many cases require specific recommendations that pertain to the type of information collected and the type of systems being used. However, there are similarities in the types of privacy risks encountered, and general best practices for risk mitigation.

For example, PIAs may only state in fairly general terms that accountability for protecting personal information “will be communicated” to staff, or that staff involved will be “made aware of” their responsibilities. The OPC prefers a much more specific and proactive approach, and has recommended the issuance of binding guidelines, protocols and well documented procedures.

Similarly, PIAs submitted to us may not include a process for the departments or agencies to inform affected individuals if personal information has been found to be inappropriately disclosed either accidentally or as a result of theft. We recommend that every department have a clear policy in place to guide managers and other staff in instances where personal information has gone astray.

Other examples of common recommendations to help mitigate privacy risks include:

- Asking government institutions to ensure that privacy protections are built into contracts for processing or storing personal information, including regular departmental audits of contractors' practices
- Recommending the inclusion of clear acknowledgement of responsibility for safeguarding personal information in service agreements
- Ensuring that PIA summaries are written in clear, non-technical language and that they are posted on departmental web sites
- Reminding institutions of their obligation to amend personal information banks to reflect new information being collected, or new uses for that information, as required under the *Privacy Act*

- Training all staff in privacy protective work habits, and ensuring that all office procedures are compliant with the *Privacy Act*
- Advising institutions to monitor the transaction logging programs that are in place to protect against unauthorized access to personal information

As a particular issue, the OPC notes a trend of increased sharing of information among police and national security agencies for law enforcement and anti-terrorism purposes. Several of the PIAs reviewed could be grouped into these categories. A concern is that this Office receives privacy assessments of large and potentially privacy invasive projects in disjointed pieces, rather than as part of a comprehensive overview. The OPC has recommended to entities such as Transport Canada, the CBSA and the RCMP that an overall privacy management framework and/or a comprehensive PIA be developed at the outset of such large, integrated projects.

The trend towards government institutions forming integrated networks to share personal information creates new privacy challenges. When several departments and agencies feed data into a network that is accessible to partners that span across jurisdictions, issues of governance, custody and control of information arise, as do issues around consent, right of access and correction.

The OPC will continue monitoring some of the large-scale projects through PIA review and updates, including the expansion of the Canadian Public Safety Information Network (CPISN). This initiative, which falls under Public Safety and Emergency Preparedness Canada (PSEPC), seeks to establish a national information sharing network for Canada's criminal justice system and law enforcement agencies, linking previously separated sources of data related to crime and offenders. The OPC will also monitor projects that collect and analyze the personal information of travelling individuals collected at border points and from passenger reservation systems.

As part of a privacy management framework, the OPC will continue encouraging departments to establish a formal administrative structure such as an internal committee or working group that is specifically responsible for reviewing departmental initiatives to determine whether they require a PIA, and for implementing privacy risk reduction measures after a PIA has been done. The OPC is actively considering undertaking an audit of the government-wide PIA system in order to establish whether institutions are doing PIAs when they should, are following up on risk assessment findings, and fixing privacy protection gaps when identified.

Other Work

Following are other audit and review projects from the past fiscal year.

Statistics Canada Census

Statistics Canada has been consulting this Office regarding the 2006 Census for the past several years. One new dimension for the Census was a proposal to rely on services of a third party contractor. In response to concerns of this Office and others about initially proposed contracting arrangements with a company based in a foreign jurisdiction, Statistics Canada significantly revised its approach to ensure that no census data would reside outside of the department.

Our monitoring of Census preparation included document review and a visit to the Data Processing Centre (DPC) of Statistics Canada. Based on this, we are satisfied that reasonable precautions are being taken to ensure the integrity and confidentiality of Census data. In addition to contract and policy means, these measures include independent IT security assessment of DPC, a threat risk assessment, and control of traffic in and out of the DPC. We did point out the need to amend documented procedures to clarify for the purpose of the 2006 Census that there should be no remote access to the DPC.

Canada Post Track-a-Package

In 2005 we investigated apparent vulnerabilities regarding Canada Post Corporation's (CPC) web-based Track-a-Package service. As a result, CPC agreed to undertake several practice improvements. This included procedures to authenticate the identity of clients requesting information, means to inform customers that their signature will be available on the internet and ensuring that their signature does not appear for registered mail when a customer objects to this, and ways of reminding customers of the importance of protecting their PIN.

Disclosure of certain personal information on CRTC web site

In response to concerns communicated to our Office about the Canadian Radio-television and Telecommunications Commission (CRTC) publishing on its web site the personal contact information of interveners in public proceedings, we engaged with the CRTC in reaching reasonable solutions regarding notification and limiting access to such information.

IN THE COURTS

Privacy Act Applications

Once the Office of the Privacy Commissioner has investigated a complaint, section 41 of the *Privacy Act* allows the individual to apply to the Federal Court for review of the government's refusal to provide access to personal information. The following applications and appeals were filed in the past fiscal year. In keeping with our mandate, we have chosen not to reproduce the official style of cause of the cases in order to respect the privacy of the individual complainants. We are listing the court docket number and the name of the government institutions only.

Président de l'Agence spatiale canadienne

Federal Court File No.: T-1448-05

Solicitor General of Canada

Federal Court File No.: T-1724-05

Minister of Public Safety and Emergency Preparedness

Federal Court File No.: T-2123-05

Royal Canadian Mounted Police

Federal Court File No.: T-66-06

Solicitor General of Canada

Federal Court of Appeal File No.: A-111-05

Minister of National Revenue

Federal Court of Appeal File No.: A-270-05

Section 42 of the *Privacy Act* also allows the Commissioner to appear in Federal Court. The Commissioner may ask the Court to review an institution's refusal of access to personal information (with the complainant's consent). She may act on behalf of individuals who have applied for review themselves, or with the leave of the Court, be a party to any review sought under section 41. No such situation arose in the past fiscal year.

Judicial Review

Complainants will sometimes seek judicial review under section 18.1 of the *Federal Courts Act* against the Privacy Commissioner. This occurred in the case described below, where the Commissioner was required to explain her jurisdiction to the Court when the complainant sought remedies that the Commissioner had no authority to grant. This case illustrates the seriously limited remedies available under the *Privacy Act* for any breaches other than improper denials of access. The Commissioner finds herself in the unenviable position of having to demonstrate to the Court how she is unable to help the complainant. Clearly, this is an important issue for reform of the *Privacy Act*, which is discussed earlier in this report.

Royal Canadian Mounted Police and Privacy Commissioner of Canada

Federal Court File No.: T-1180-04 and Federal Court of Appeal File No.: A-183-05

The applicant complained to the Privacy Commissioner, that among other wrongful conduct, the RCMP had breached the *Privacy Act* by disclosing his personal information to his employer without his consent. The Assistant Commissioner responsible for the *Privacy Act* agreed that his disclosure complaint was well-founded, but indicated that, unfortunately, no remedy exists for such disclosures under the Act.

On June 18, 2004, the applicant sought a judicial review of the Assistant Commissioner's report on his disclosure complaint. Although the *Privacy Act* restricts remedies to questions of access, he argued that the Privacy Commissioner must necessarily have the authority to fashion remedial orders and relief in cases (like his) where the *Privacy Act* has been contravened.

In a decision dated March 29, 2005, the Court determined that the Privacy Commissioner had fulfilled her obligations under the *Privacy Act* and had correctly advised the applicant that the *Privacy Act* provides no remedy to address the

respondent's breach of his privacy. The applicant can obtain no further relief in the Court for the improper disclosure.

The applicant appealed the Federal Court decision in April 2005, but discontinued the appeal a few weeks prior to the scheduled appeal hearing.

PUBLIC EDUCATION AND COMMUNICATIONS

The Office of the Privacy Commissioner of Canada is mandated specifically under *PIPEDA* to educate the public and organizations on rules that govern the collection, use and disclosure of personal information in the course of commercial activities. Although there is no specified mandate for public education and communications under the *Privacy Act*, clearly it is necessary to communicate with government institutions about the application of the Act and the implications of their actions on the privacy rights of Canadians, so they can be held accountable for their personal information handling practices. There is also an expectation for the Commissioner and her Office to comment publicly on federal government initiatives involving personal information.

Public Opinion Polling

In 2004-2005, the Office developed a comprehensive communications and outreach strategy for the coming fiscal years. One of the initiatives in this strategy involved public opinion research, so that we could better understand how Canadians view privacy issues, as well as their levels of awareness. A majority of Canadians surveyed expressed a strong sense that their privacy and protection of their personal information was being eroded. Among other findings of particular interest, Canadians expressed concern about the transborder flow of personal information and expressed lower confidence in new technology, especially in the area of electronic health records. Respondents were also of the view that privacy laws should be updated to address the rapid evolution of information technology. This past fiscal year (2005-06), we conducted a follow-up study. The findings suggest that the concerns outlined above are still very present, and also that privacy laws must be updated to keep pace with leading-edge, transformational technologies that have a significant impact on privacy. A report on the latest study will be posted to our Web site in the summer of 2006.

Speeches and Special Events

Speaking engagement opportunities have helped our Office promote privacy issues among diverse audiences and settings across Canada and abroad, including to professional and industry associations, non-profit and advocacy groups and universities. In the 2005-2006 fiscal year, the Commissioner, Assistant Commissioners and other senior officials delivered approximately 40 speeches. Our Office also continued to host an in-house Privacy Lecture Series approximately once a month. Privacy experts from Canada and abroad shared their observations on a wide range of issues with an internal and external audience of stakeholders.

Media Relations

Privacy issues continued to be of interest to the media in 2005-2006, with media coverage in Canada on issues such as government initiatives with privacy implications, privacy breaches, as well as surveillance technologies. These areas generated numerous media calls to and interviews with OPC officials. In addition, through other proactive media relations efforts, such as the dissemination of news releases, the Commissioner had an opportunity to share her views on federal government legislation and initiatives, such as the Passenger Project or the “No-Fly List”, and the Office’s views regarding transborder flows of personal information.

Web Site

The Office frequently posts new and useful information to its web site. Fact sheets, news releases, speeches, reports and publications, and case summaries of findings under the federal private sector law are posted to keep the site relevant to individuals and institutions. Since 2001-2002, we are pleased to report that visits to the site have more than quadrupled, and that we surpassed the one million visitors’ mark in the 2005-2006 fiscal year.

Publications

Each year, the OPC produces and disseminates publications to individuals and organizations seeking information on privacy matters. These documents include annual reports, guides, as well as fact sheets and copies of both federal statutes. Not only were these materials sent to individuals upon request, they were also distributed at conferences and special events. Increasingly, individuals are also accessing these documents on our web site.

Internal Communications

Internal communications activities were also a focus of the Office in 2005-2006, increasing transparency between management and staff, especially throughout the Office's institutional renewal. Internal communications activities in 2005-2006 involved providing information on issues such as human resources, upcoming speaking engagements, Parliamentary appearances, senior management and labour management committee meetings, and special events. In 2005-2006 the Office also launched its Intranet site which serves as the internal communications portal, maximizing staff access to information.

Although public education and communications are an important part of our work, limited financial and human resources have constrained our ability to go much beyond simply responding to issues, rather than anticipating them and preparing public education strategies in advance. We have also discussed this in our recently tabled 2005 Annual Report to Parliament on *PIPEDA*. However, expected increases in funding will permit us to not only undertake the activities outlined above, but to undertake more extensive public awareness initiatives and to carry out the comprehensive proactive communications and outreach strategy mentioned earlier in this chapter.

CORPORATE SERVICES

The Commissioner continues to focus on effective management renewal. During 2005-06, the main priority was the completion of the business case seeking long-term permanent resources. A second priority was strengthening our Human Resources management capacity.

Planning and Reporting

A foundation component of the Office's institutional renewal is a strategic planning, reporting and control process. In 2005-06 we completed our second year under this revised process. The strategic plan established at the beginning of the year was our road map for the year. One important part of the new process was reporting and review opportunities. We reviewed and made adjustments to plans and budgets throughout the year. To assist in our reporting, we continued work on our Performance Measurement Framework and our monthly performance report has been in place for 18 months. This serves as a critical management tool for the evaluation of branch results against targets.

Human Resources

We continue to work toward the development and implementation of changes to improve how the Office is run and the overall quality of the workplace. Significant changes and improvements have been made to the Human Resource management policies and practices.

We have implemented a number of Human Resource policies in consultation with central agencies and unions in line with the new *Public Service Employment Act* (PSEA) requirements. These policies will guide us as we build on the successes of the past year and as we continue on our path of institutional renewal. An Instrument

of Delegation of Human Resource Management was developed and will serve as a tool to inform and guide managers, and enable them to manage their human resources. A Strategic Human Resource Plan and a new Staffing Strategy, as well as an Employment Equity Action Plan, will help the OPC achieve its mandate and will ensure the recruitment of a highly qualified workforce that is diversified and representative of Canadian society. As part of the OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed on a monthly basis to all staff.

We made significant strides in the area of organizational learning, including the development of a learning strategy with the Canada School of Public Service (CSPS), training and information sessions in areas such values-based staffing, language, performance management, employee appraisals, and harassment awareness in the workplace. We have provided briefing sessions at our quarterly all-staff meetings, as well as to all managers on various aspects of the new PSMA and PSEA. The Learning Strategy and Curriculum with the CSPS enables staff to continue to develop the expertise and competencies required to fulfill their functions, which will position them to take on their new responsibilities and accountabilities. The learning strategy has been modified to reflect training requirements related to the new PSEA, including a Senior Management Committee Engagement Session and PSEA training for sub-delegated managers, both of which were offered in March 2006.

We continue to work collaboratively with the Public Service Commission and the Public Service Human Resources Management Agency of Canada on follow-up measures to the recommendations of their audit reports. This includes measures that will allow OPC the opportunity to regain its full staffing delegation authority.

Finance and Administration

The OPC received a clean opinion on Audited 2004-2005 Financial Statements by the Office of the Auditor General of Canada. Combined with the 2003-2004 clean opinion, this is a very positive indicator that the organization has indeed advanced on the path of institutional renewal. The organization has built on that success by establishing planning and review cycles, and by streamlining and improving the financial management policies and practices of the OPC.

Information Management / Information Technology

The IM/IT Division has accomplished many things over the past year. We have renewed our server infrastructure and increased data storage to allow for the scanning of documents. Good progress has been made on our Information Management project. Upgrades to our records management and correspondence tracking systems have been completed. Financial systems – Salary Management System (SMS) and FreeBalance - have been upgraded and the FreeBalance server has been upgraded as well. Five new tracking systems have been developed for the Audit and Review Branch to allow them to track their Audit files. We have completed the Action Plan for MITS Compliance and we are working steadily towards the December 2006 compliance deadline.

Our Resource Needs

As described in an earlier section of this report, the Office completed a thorough analysis that included a business process review of all OPC functions. Following that review we requested more than a fifty percent increase in resources which will bring our overall budget to approximately \$18 million dollars and our full-time equivalents (FTEs) to a total of 140 over the course of the next two years. There will also be a shift in the relative distribution of resources to position the organization to be more proactive as opposed to reactive.

Financial Information

In past years the Annual Report was often produced later. This allowed us to provide financial tables relating to our expenditures at that time. The normal financial reporting cycle does not allow us to provide audited financial statements at the time of tabling this report. We will provide financial information in our Reports on Plans and Priorities, as well as our Departmental Performance Reports, both of which are tabled in Parliament. Furthermore, as we have in the past, we will also post to our web site the Audited Financial Statements for fiscal year 2005-06 once they are completed. For additional financial information, we encourage you to visit our web site at www.privcom.gc.ca.

APPENDIX 1

Access and Privacy Complaints Closed by Institution and Finding From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded – Resolved	Total
Bank of Canada	0	0	1	0	0	0	0	1
Canada Border Services Agency	1	0	4	1	1	0	0	7
Canada Customs and Revenue Agency	5	0	4	0	8	0	1	18
Canada Post Corporation	28	0	4	0	6	1	0	39
Canada Revenue Agency	0	2	30	2	6	2	1	43
Canadian Food Inspection Agency	0	0	0	1	0	0	0	1
Canadian Human Rights Commission	0	0	0	1	1	0	0	2
Canadian Nuclear Safety Commission	0	0	1	0	0	0	0	1
Canadian Security Intelligence Service	15	0	35	0	1	0	0	51
Canadian Space Agency	0	0	2	0	0	0	2	4
Citizenship and Immigration Canada	6	0	7	0	10	1	3	27

Access and Privacy Complaints Closed by Institution and Finding (cont.)

From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded – Resolved	Total
Correctional Investigator	1	0	0	0	0	1	0	2
Correctional Service Canada	27	11	40	3	22	14	3	120
Farm Credit Canada	0	0	1	0	0	0	0	1
Fisheries and Oceans	1	0	3	0	1	0	0	5
Foreign Affairs and International Trade Canada	0	0	2	0	0	0	1	3
Health Canada	0	0	2	0	4	0	0	6
Human Resources and Skills Development Canada	0	3	5	0	9	1	2	20
Immigration and Refugee Board	0	0	8	0	1	0	1	10
Indian and Northern Affairs Canada	0	0	2	0	0	0	0	2
Industry Canada	0	0	1	0	0	0	0	1
Justice Canada, Department of	0	0	11	0	3	0	2	16
Library and Archives Canada	0	0	0	0	3	0	0	3
Military Police Complaints Commission	0	0	1	0	0	0	0	1
National Capital Commission	0	0	0	0	4	0	0	4
National Defence	1	0	1	2	3	2	1	10
National Gallery of Canada	1	0	0	0	0	0	0	1
National Parole Board	0	0	1	0	2	1	0	4

Access and Privacy Complaints Closed by Institution and Finding (cont.)

From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded – Resolved	Total
National Research Council Canada	0	0	0	0	1	0	2	3
Natural Sciences and Engineering Research Council of Canada	0	0	0	0	1	0	0	1
Office of the Commissioner of Official Languages	0	0	0	0	0	0	1	1
Office of the Chief Electoral Officer	0	0	10	0	1	0	0	11
Pacific Pilotage Authority Canada	0	0	0	0	0	0	1	1
Pension Appeals Board Canada	0	0	0	0	1	0	0	1
Privy Council Office	0	0	1	0	0	0	0	1
Public Service Commission Canada	0	0	0	0	1	3	0	4
Public Works and Government Services Canada	0	0	1	1	0	0	0	2
Royal Canadian Mounted Police	5	0	36	4	12	1	1	59
Social Development Canada	1	0	3	0	4	0	0	8
Statistics Canada	0	0	0	0	2	1	0	3
Transport Canada	0	1	0	0	0	0	0	1
Treasury Board Secretariat	0	0	1	0	0	0	1	2
Veterans Affairs Canada	0	0	0	0	2	0	0	2
Total	92	17	218	15	110	28	23	503

APPENDIX 2

Time Limit Complaints Closed by Institution and Finding From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Total
Canada Border Services Agency	0	0	0	0	0	11	11
Canada Post Corporation	16	0	0	0	0	0	16
Canada Revenue Agency	4	0	7	10	0	17	38
Canadian Air Transport Security Authority	0	0	0	0	0	1	1
Canadian Food Inspection Agency	1	0	0	0	0	0	1
Canadian Security Intelligence Service	0	0	4	0	0	1	5
Citizenship and Immigration Canada	2	0	1	0	0	55	58
Correctional Service Canada	2	1	3	0	1	54	61
Environment Canada	0	0	0	0	0	1	1
Export Development Corporation	0	1	0	0	0	0	1

Time Limit Complaints Closed by Institution and Finding (cont.)

From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Total
Foreign Affairs and International Trade Canada	0	0	6	0	1	20	27
Health Canada	0	0	0	0	0	9	9
Human Resources and Skills Development Canada	0	0	2	0	0	2	4
Immigration and Refugee Board	15	0	6	0	4	98	123
Industry Canada	0	1	0	0	0	0	1
Justice Canada	1	0	2	0	0	6	9
Library and Archives Canada	0	0	0	0	0	1	1
National Archives of Canada	0	0	0	0	0	1	1
National Defence	4	0	1	0	0	18	23
National Gallery of Canada	0	1	0	0	0	0	1
National Research Council Canada	0	0	23	0	0	23	46
Privy Council Office	0	0	0	0	0	2	2
Public Service Commission Canada	0	0	2	0	0	0	2
Public Works and Government Services Canada	0	0	1	0	0	1	2
Royal Canadian Mounted Police	4	0	1	1	2	83	91
Transport Canada	0	2	0	0	0	0	2
Total	49	6	59	11	8	404	537

Plaintes fermées par institution gouvernementale et par conclusions d'enquête
 reliées au délai (suite)
 Entre le 1^{er} avril 2005 et le 31 mars 2006

Reportant	Abandonnée	Réglée rapidement	Non fondée	Réglée	Réglée en cours d'enquête	Fondée	Total
-----------	------------	-------------------	------------	--------	---------------------------	--------	-------

Exportation et Développement Canada	0	1	0	0	0	0	1
Gendarmerie royale du Canada	4	0	1	1	2	83	91
Industrie Canada	0	1	0	0	0	0	1
Justice Canada	1	0	2	0	0	6	9
Musée des beaux-arts du Canada	0	1	0	0	0	0	1
Ressources humaines et Développement des compétences Canada	0	0	2	0	0	2	4
Santé Canada	0	0	0	0	0	9	9
Service canadien du renseignement de sécurité	0	0	4	0	0	1	5
Service correctionnel Canada	2	1	3	0	1	54	61
Société canadienne des postes	16	0	0	0	0	0	16
Transports Canada	0	2	0	0	0	0	2
Travaux publics et Services gouvernementaux Canada	0	0	1	0	0	1	2
Total	49	6	59	11	8	404	537

Plaintes fermées par institution gouvernementale et par conclusions d'enquête
 reliées au délais
 Entre le 1^{er} avril 2005 et le 31 mars 2006

Repondant	Abandonnée	Réglée rapidement	Non fondée	Résolue	Réglée en cours d'enquête	Fondée	Total
-----------	------------	-------------------	------------	---------	---------------------------	--------	-------

Agence canadienne d'inspection des aliments	1	0	0	0	0	0	1
Agence des services frontaliers du Canada	0	0	0	0	0	11	11
Agence du revenu du Canada	4	0	7	10	0	17	38
Administration canadienne de la sûreté du transport aérien	0	0	0	0	0	1	1
Affaires étrangères et Commerce international	0	0	6	0	1	20	27
Archives nationales du Canada	0	0	0	0	0	1	1
Bibliothèque et Archives Canada	0	0	0	0	0	1	1
Bureau du Conseil privé	0	0	0	0	0	2	2
Citoyenneté et Immigration Canada	2	0	1	0	0	55	58
Commission de l'immigration et du statut de réfugié du Canada	15	0	6	0	4	98	123
Commission de la fonction publique du Canada	0	0	2	0	0	0	2
Conseil national de recherches Canada	0	0	23	0	0	23	46
Défense nationale	4	0	1	0	0	18	23
Environnement Canada	0	0	0	0	0	1	1

Plaintes fermées par institution gouvernementale et par conclusions d'enquête
 reliées à l'accès et à la protection des renseignements personnels (suite)
 Entre le 1^{er} avril 2005 et le 31 mars 2006

APPENDIX I

Reportant	Abandonnée	Réglée rapidement	Non fondée	Réglée	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
Ressources humaines et Développement des compétences Canada	0	3	5	0	9	1	2	20
Santé Canada	0	0	2	0	4	0	0	6
Secrétariat du Conseil du Trésor	0	0	1	0	0	0	1	2
Service canadien du renseignement de sécurité	15	0	35	0	1	0	0	51
Service correctionnel Canada	27	11	40	3	22	14	3	120
Société canadienne des postes	28	0	4	0	6	1	0	39
Statistique Canada	0	0	0	0	2	1	0	3
Transports Canada	0	1	0	0	0	0	0	1
Travaux publics et Services gouvernementaux Canada	0	0	1	1	0	0	0	2
Total	92	17	218	15	110	28	23	503

Plaintes fermées par institution gouvernementale et par conclusions d'enquête
relées à l'accès et à la protection des renseignements personnels (suite)
Entre le 1^{er} avril 2005 et le 31 mars 2006

Repondant	Abandonnée	Réglée rapidement	Non fondée	Réglée en cours	Fondée	Fondée et résolue	Total
-----------	------------	-------------------	------------	-----------------	--------	-------------------	-------

Commissariat aux langues officielles	0	0	0	0	0	1	1
Commission canadienne de sûreté nucléaire	0	0	1	0	0	0	1
Commission canadienne des droits de la personne	0	0	0	1	1	0	2
Commission d'appel des pensions	0	0	0	0	1	0	1
Commission d'examen des plaintes concernant la police militaire	0	0	1	0	0	0	1
Commission de l'immigration et du statut de réfugié du Canada	0	0	8	0	1	0	10
Commission de la capitale nationale	0	0	0	0	4	0	4
Commission de la fonction publique du Canada	0	0	0	0	1	3	4
Commission nationale des libérations conditionnelles	0	0	1	0	2	1	4
Conseil de recherches en sciences naturelles et en génie	0	0	0	0	1	0	1
Conseil national de recherches Canada	0	0	0	0	1	0	3
Défense nationale	1	0	1	2	3	2	10
Développement social Canada	1	0	3	0	4	0	8
Financement agricole Canada	0	0	1	0	0	0	1
Gendarmerie royale du Canada	5	0	36	4	12	1	59
Industrie Canada	0	0	1	0	0	0	1
Justice Canada	0	0	11	0	3	0	16
L'Enquêteur correctionnel Canada	1	0	0	0	0	1	2
Musée des beaux-arts du Canada	1	0	0	0	0	0	1
Pêches et Océans Canada	1	0	3	0	1	0	5

Plaintes fermées par institution gouvernementale et par conclusions d'enquête
 reliées à l'accès et à la protection des renseignements personnels
 Entre le 1^{er} avril 2005 et le 31 mars 2006

Repondant	Abandonnée	Réglée rapidement	Non fondée	Réglée en cours	Fondée	Fondée et résolue	Total
-----------	------------	-------------------	------------	-----------------	--------	-------------------	-------

Administration de pilotage du Pacifique Canada	0	0	0	0	0	0	1
Affaires étrangères et Commerce international	0	0	2	0	0	0	3
Affaires indiennes et du Nord Canada	0	0	2	0	0	0	2
Agence canadienne d'inspection des aliments	0	0	0	1	0	0	1
Agence des douanes et du revenu du Canada	5	0	4	0	8	0	18
Agence des services frontaliers du Canada	1	0	4	1	1	0	7
Agence du revenu du Canada	0	2	30	2	6	2	43
Agence spatiale canadienne	0	0	2	0	0	0	4
Anciens combattants Canada	0	0	0	0	2	0	2
Banque du Canada	0	0	1	0	0	0	1
Bibliothèque et Archives Canada	0	0	0	0	3	0	3
Bureau du Conseil privé	0	0	1	0	0	0	1
Bureau du directeur général des élections	0	0	10	0	1	0	11
Citoyenneté et Immigration Canada	6	0	7	0	10	1	27

des états financiers vérifiés au moment où nous présentons ce rapport annuel. Nous fournirons l'information financière dans les rapports sur les plans et les priorités ainsi que dans nos rapports ministériels sur le rendement, tous deux à l'intention du Parlement. De plus, nous afficherons sur notre site Web, comme par les années passées, les états financiers vérifiés pour l'exercice 2005-2006 des que ceux-ci seront complétés. Pour en savoir davantage sur la question des finances du Commissariat, prière de consulter notre site Web, à l'adresse suivante : www.privcom.gc.ca.

Finances et administration

Le Bureau du vérificateur général du Canada a communiqué une opinion sans réserve au Commissariat concernant les états financiers vérifiés de 2004-2005. Compte tenu de l'opinion sans réserve formulée en 2003-2004, c'est un signe très positif de nos progrès en matière de renouvellement institutionnel. Nous nous sommes appuyés sur ces résultats pour créer des cycles de planification et d'examen et simplifier et améliorer les politiques et pratiques de gestion financière du Commissariat.

Gestion et technologie de l'information

La Division GI/TI a accompli beaucoup de travail au cours du dernier exercice. Nous avons renouvelé notre infrastructure de serveur et augmenté notre capacité de stockage de données pour permettre le scannage de documents. Nous avons marqué des progrès dans le cadre du projet de gestion de l'information. Nous avons terminé la mise à jour de nos systèmes de gestion des documents et de repérage de la correspondance. Les systèmes financiers (système de gestion des salaires et FreeBalance) ont été mis à niveau, et le serveur FreeBalance a été, lui aussi, mis à niveau. Cinq nouveaux systèmes de repérage sont en place pour la Direction générale de la vérification et de la revue afin de faciliter le repérage des dossiers de vérification. Nous avons terminé le plan d'action pour la conformité à la GSTI et nous respecterons l'échéance de décembre 2006.

Nos besoins en ressources

Tel que mentionné précédemment dans ce rapport, le Commissariat a procédé à une analyse approfondie de son fonctionnement, dont un examen des procédures opérationnelles associées à toutes ses fonctions. Après quoi, nous avons demandé une augmentation de ressources de plus de cinquante pour cent, pour amener notre budget global à environ 18 millions de dollars et nos équivalents temps plein (ETP) à un total de 140 au cours des deux prochaines années. Les ressources seront réparties différemment pour faire du Commissariat un organisme plus proactif.

Information financière

Au cours des années précédentes, le rapport annuel était souvent réalisé plus tardivement; nous pouvions donc y inclure des tableaux financiers de nos dépenses. Le cycle normal d'établissement des rapports financiers ne nous permet pas de fournir

Nous avons mis en œuvre un certain nombre de politiques en matière de ressources humaines, après consultation auprès des organismes centraux et des syndicats et dans le respect des dispositions de la *Loi sur l'emploi dans la fonction publique* (LEFP). Ces politiques nous orienteront dans la démarche fructueuse entamée au cours de l'exercice précédent et dans la suite du renouvellement institutionnel. Nous avons élaboré un outil de délégation de la gestion des ressources humaines qui servira à informer et orienter les gestionnaires et à leur permettre de gérer les ressources humaines qui relèvent d'eux. Le plan de gestion stratégique des ressources humaines et la nouvelle stratégie de dotation en personnel ainsi que le plan d'action pour l'équité en matière d'emploi contribueront à la réalisation du mandat du Commissariat et garantiront le recrutement d'un personnel hautement qualifié, diversifié et représentatif de la société canadienne. Dans le cadre de l'engagement du Commissariat à accroître la transparence des procédures de dotation en personnel, nous avons créé un bulletin d'information à l'intention du personnel : il est distribué tous les mois à l'ensemble des employés.

Nous avons fait beaucoup de progrès dans le domaine de l'apprentissage organisationnel, notamment grâce à l'élaboration d'une stratégie d'apprentissage de concert avec l'École de la fonction publique du Canada (EFPC), à des ateliers de formation et d'information sur la dotation axée sur les valeurs, les langues officielles, la gestion du rendement, l'évaluation des employés, la sensibilisation au harcèlement en milieu de travail, etc. Nous avons organisé des séances d'information à l'occasion des réunions trimestrielles du personnel et à l'intention des gestionnaires sur tous les aspects des nouvelles LMFP et LEFP. La stratégie et le programme d'apprentissage de l'EFPC permettent au personnel de développer l'expertise et les compétences nécessaires à l'exécution de leurs tâches et d'être en mesure d'assumer de nouvelles responsabilités. La stratégie d'apprentissage a été modifiée en fonction des besoins en formation relatifs à la nouvelle LEFP ; nous avons notamment offert une formation participative pour le comité de la haute direction et une formation sur la LEFP pour les gestionnaires assumant des responsabilités déléguées (les deux ont eu lieu en mars 2006).

Nous continuons de collaborer avec la Commission de la fonction publique et l'Agence de gestion des ressources humaines de la fonction publique concernant le suivi des recommandations contenues dans leurs rapports de vérification. Il s'agit, entre autres, de prendre des mesures permettant au Commissariat de récupérer intégralement son pouvoir de délégation de la fonction de dotation.

7 a commissaire continue de s'intéresser au renouvellement efficace du système de gestion. Au cours de l'exercice 2005-2006, la priorité à cet effet fut de terminer l'analyse de rentabilisation en vue d'obtenir un financement permanent et à long terme. La seconde priorité fut de consolider notre capacité de gestion des ressources humaines.

Planification et reddition des comptes

L'un des piliers du renouvellement institutionnel du Commissariat est le processus stratégique de planification, de reddition des comptes et de contrôle. En 2005-2006, nous avons clôturé la deuxième année de fonctionnement de ce processus. Le plan stratégique dressé au début de l'année constituait notre feuille de route pour tout l'exercice. Profiter des occasions de réaliser examens et redditions des comptes est un volet important du nouveau processus. Nous avons examiné et adapté nos plans et nos budgets tout au long de l'année à cet effet. Pour favoriser la reddition de comptes, nous avons continué à développer le cadre d'évaluation du rendement, et nous procédons au rapport de rendement mensuel depuis 18 mois. Il s'agit d'un outil de gestion crucial à l'évaluation des résultats des directions générales en fonction de leurs objectifs.

Les ressources humaines

Nous continuons d'élaborer et de mettre en œuvre des mesures pour améliorer le fonctionnement du Commissariat et la qualité générale du milieu de travail. Des modifications et améliorations importantes ont été apportées aux politiques et aux pratiques de gestion des ressources humaines.

présentent plutôt que de les anticiper et d'élaborer des stratégies de sensibilisation en conséquence. Nous avons déjà émis ces commentaires dans le rapport annuel sur la *LPRPDE* (2005) déposé au Parlement. Néanmoins, l'augmentation prévue du financement nous permettra non seulement de mener à bien les fonctions ci-haut mentionnées, mais de mettre en œuvre des initiatives de conscientisation du grand public à portée plus vaste et de concrétiser la stratégie exhaustive et proactive de communication et de rayonnement dont il a été question plus haut.

d'interdiction aériennes) ainsi que de faire valoir le point de vue du Commissariat sur la circulation transfrontalière de renseignements personnels.

Le site Web

Le Commissariat affiche régulièrement sur son site Web de l'information sur ses dernières activités et de l'information pratique. Des fiches de renseignements, des communiqués de presse, des discours, des rapports et des publications ainsi que des résumés de conclusions d'enquêtes en vertu de la loi fédérale s'appliquant au secteur privé sont affichés afin que le site demeure une source efficace de renseignements pour les personnes et les institutions. Nous constatons avec plaisir que depuis 2001-2002 le nombre de consultations a plus que quadruplé et que nous avons passé le seuil d'un million de consultations au cours de l'exercice 2005-2006.

Les publications

Chaque année, le Commissariat produit et fait paraître des documents destinés aux personnes et aux organismes qui s'intéressent aux questions relatives à la protection de la vie privée. Il peut s'agir de rapports annuels, de guides, de fiches de renseignements et d'exemplaires des deux lois fédérales applicables. Non seulement faisons-nous parvenir ces documents aux personnes qui en font la demande, mais nous les distribuons à l'occasion de conférences et d'événements spéciaux. Les gens les consultent également de plus en plus sur notre site Web.

Les communications internes

Les communications internes ont également fait l'objet de notre attention au cours de l'exercice 2005-2006 dans le but d'accroître la transparence des relations entre la direction et le personnel, notamment dans le cadre du renouvellement institutionnel du Commissariat. Il s'agissait de fournir de l'information sur des questions se rapportant aux ressources humaines, aux allocutions éventuelles, aux comparutions devant le Parlement, aux réunions du comité de direction et du comité de consultation patronale-syndicale ainsi qu'aux événements spéciaux. En 2005-2006, le Commissariat a également lancé son site intranet, qui sert de portail des communications internes et permet de maximiser l'accès du personnel à l'information.

La sensibilisation du grand public et les communications sont un volet important de notre travail, mais les ressources humaines et financières dont nous disposons à cet effet sont restreintes et nous limitent généralement à réagir aux situations qui se

la circulation transfrontalière de renseignements personnels et fait peu confiance aux nouvelles technologies, notamment en ce qui concerne les dossiers électroniques de santé. Les personnes interrogées étaient également d'avis que les lois en matière de protection de la vie privée devraient être mises à jour de façon à ce qu'elles tiennent compte de l'évolution rapide de la technologie de l'information. Au cours du dernier exercice (2005-2006), nous avons procédé à une étude de suivi; selon les résultats obtenus, il appert que les préoccupations formulées précédemment demeurent très actuelles et que les lois sur la protection de la vie privée doivent être mises à jour afin d'emboîter le pas aux technologies transformationnelles de pointe qui ont une incidence considérable sur la protection de la vie privée. Le compte rendu de la dernière étude sera affiché sur notre site Web au cours de l'été 2006.

Discours et événements spéciaux

Le Commissariat a profité de nombreuses occasions de prononcer des allocutions pour promouvoir les enjeux en matière de protection de la vie privée auprès de divers auditoires au Canada et à l'étranger, notamment auprès d'associations professionnelles et industrielles, de groupes sans but lucratif, de groupes de revendications et d'universitaires. Au cours de l'exercice 2005-2006, la commissaire et les deux commissaires adjoints, ainsi que d'autres hauts fonctionnaires, ont prononcé une quarantaine de discours.

Le Commissariat a continué de présenter sa série de conférences internes sur la protection de la vie privée, à raison d'une conférence par mois environ. Des spécialistes canadiens et étrangers de la protection de la vie privée y ont participé et ont fait part, à des auditoires internes et externes, de leurs points de vue sur des questions variées.

Les relations avec les médias

Les médias se sont intéressés aux enjeux en matière de protection de la vie privée au cours de l'exercice 2005-2006; au Canada, les médias ont couvert des sujets se rapportant aux mesures gouvernementales ayant des répercussions sur la vie privée, aux atteintes à la protection de la vie privée, et aux technologies de surveillance. Les personnes désignées du Commissariat ont été grandement sollicitées par les médias à cet égard et ont accordé plusieurs entrevues. Par ailleurs, grâce à d'autres mesures proactives, telle la diffusion de communiqués, la commissaire a eu l'occasion de faire part de ses observations sur la réglementation et les initiatives du gouvernement fédéral (par exemple, au sujet du Projet de passeports ou de la liste de zones

SENSIBILISATION DU GRAND PUBLIC ET COMMUNICATIONS

Le Commissariat à la protection de la vie privée du Canada a pour mandat, aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), de sensibiliser le grand public et les organisations

aux règles qui régissent la collecte, l'utilisation et la communication des renseignements personnels dans le cadre d'activités commerciales. Bien qu'aucun mandat de sensibilisation du grand public et de communications n'incombe au Commissariat en vertu de la *Loi sur la protection des renseignements personnels*, il est manifestement nécessaire de s'entretenir avec les institutions gouvernementales au sujet de l'application de la Loi et des répercussions de leurs activités sur le droit à la protection de la vie privée des Canadiennes et des Canadiens afin que ces institutions soient tenues responsables de leurs pratiques relatives aux renseignements personnels. Le Commissaire et le Commissariat ont également pour fonction de présenter publiquement leurs observations sur les initiatives du gouvernement fédéral concernant les renseignements personnels.

Les sondages d'opinion

En 2004-2005, le Commissariat a élaboré une stratégie exhaustive en matière de communications et de rayonnement pour les exercices futurs. L'une des mesures que comporte cette stratégie a trait à l'étude de l'opinion publique, dans le but de mieux comprendre la perception qu'a la population canadienne des enjeux relatifs à la protection de la vie privée, mais aussi de mieux évaluer la mesure dans laquelle elle y est consentie. Ainsi, les résultats d'un sondage indiquent que la majorité des Canadiennes et des Canadiens interrogés estiment que leur vie privée et la protection de leurs renseignements personnels se sont grandement dégradées. Entre autres constatations intéressantes, l'étude révèle que la population canadienne s'inquiète de

Le 18 juin 2004, le demandeur a adressé une demande d'examen judiciaire du rapport du commissaire adjoint sur la plainte. La *Loi sur la protection des renseignements personnels* limite les recours aux questions d'accès, mais le demandeur estimait que la commissaire à la protection de la vie privée avait nécessairement le pouvoir de rendre des ordonnances et d'ordonner des recours dans les cas (comme le sien) où la *Loi sur la protection des renseignements personnels* avait été enfreinte.

Dans une décision datée du 29 mars 2005, la Cour a conclu que la commissaire à la protection de la vie privée avait rempli ses responsabilités en vertu de la *Loi sur la protection des renseignements personnels* et qu'elle avait correctement informé le demandeur que la *Loi sur la protection des renseignements personnels* ne prévoit pas de recours dans le cas en question. Le demandeur ne peut obtenir aucune autre forme de réparation devant la Cour pour une communication non prévue par la Loi. Le demandeur a fait appel de la décision de la Cour fédérale en avril 2005, mais il a renoncé à y donner suite quelques semaines avant l'audience d'appel prévue au calendrier.

Ministre du Revenu national

Cour d'appel fédérale, numéro du greffe : A-270-05

L'article 42 de la *Loi sur la protection des renseignements personnels* autorise également la commissaire à comparaître devant la Cour fédérale. La commissaire peut demander à la Cour de procéder au contrôle judiciaire du refus d'une institution de donner accès à des renseignements personnels (avec le consentement du plaignant). Elle peut représenter des personnes ayant fait elles-mêmes une demande de contrôle judiciaire ou, si la Cour le permet, être partie à un contrôle judiciaire demandé en vertu de l'article 41. La commissaire actuelle n'a pas eu à comparaître devant la Cour, à aucun de ces titres, au cours du dernier exercice.

Le contrôle judiciaire

Les plaignants demandent parfois un contrôle judiciaire en vertu de l'article 18.1 de la *Loi sur les cours fédérales* à l'encontre d'une décision de la commissaire à la protection de la vie privée. C'est ce qui s'est produit dans le cas que nous analysons ci-dessous : la commissaire a été invitée à s'expliquer sur sa compétence après que le plaignant a demandé des mesures de réparation qui ne relevaient pas de son pouvoir. Cette cause illustre le caractère très limité des recours possibles en vertu de la *Loi sur la protection des renseignements personnels* pour toute autre atteinte à la vie privée que le refus non fondé de communiquer des renseignements. La commissaire se retrouve donc dans la position peu enviable de devoir démontrer à la Cour qu'elle n'est pas en mesure d'aider le plaignant. Cette question est manifestement importante au regard de la réforme de la *Loi sur la protection des renseignements personnels* dont nous avons parlé plus haut.

Gendarmerie royale du Canada et commissaire à la protection de la vie privée

Cour fédérale, numéro du greffe : T-1180-04

Cour d'appel fédérale, numéro du greffe : A-183-05

Le plaignant a adressé une plainte à la commissaire à la protection de la vie privée parce que, entre autres mesures illégitimes, la GRC avait enfreint la *Loi sur la protection des renseignements personnels* en communiquant des renseignements personnels le concernant sans son consentement. Le commissaire adjoint chargé de la *Loi sur la protection des renseignements personnels* s'est dit d'avis que la plainte était fondée, mais a souligné que la *Loi* ne prévoyait malheureusement aucun recours pour de telles communications.

**Demandes adressées en vertu de la
Loi sur la protection des renseignements personnels**

Après que le Commissariat à la protection de la vie privée a enquêté sur une plainte, l'article 41 de la *Loi sur la protection des renseignements personnels* autorise la personne intéressée à s'adresser à la Cour fédérale pour demander l'examen judiciaire du refus du gouvernement de lui donner accès à des renseignements personnels. Les demandes et appels suivants ont été déposés au cours du dernier exercice. Conformément à notre mandat, nous avons décidé de ne pas reproduire l'intitulé des causes tel qu'il apparaît officiellement afin de respecter la vie privée des plaignants. Nous n'énumérons que le numéro du greffe et le nom de l'institution gouvernementale en cause.

Président de l'Agence spatiale canadienne

Cour fédérale, numéro du greffe : T-1448-05

Solliciteur général du Canada

Cour fédérale, numéro du greffe : T-1724-05

Ministre de la Sécurité publique et de la Protection civile

Cour fédérale, numéro du greffe : T-2123-05

Gendarmerie royale du Canada

Cour fédérale, numéro du greffe : T-66-06

Solliciteur général du Canada

Cour d'appel fédérale, numéro du greffe : A-111-05

La communication de certains renseignements personnels sur le site Web du CRTC

En réponse aux préoccupations adressées au Commissariat au sujet de la décision du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) d'afficher sur son site Web les coordonnées d'intervenants dans des audiences publiques, nous avons invité le Conseil à prendre des mesures raisonnables concernant les avis et pour limiter l'accès à ces renseignements.

pour déterminer si les institutions réalisent les EFPV lorsque nécessaire, procèdent au suivi des conclusions relatives aux évaluations des risques, et comblent les manquements à la protection de la vie privée qui ont été identifiés.

Autres activités

Voici d'autres projets de vérification et d'examen réalisés au cours du dernier exercice.

Le recensement de Statistique Canada

Statistique Canada nous consulte depuis plusieurs années au sujet du recensement de 2006. L'un des nouveaux aspects du recensement était le projet de faire appel aux services d'un entrepreneur. Compte tenu des préoccupations formulées par le Commissariat et d'autres intervenants concernant des dispositions d'abord envisagées avec une entreprise dont le siège social se trouvait à l'étranger, Statistique Canada a modifié considérablement sa méthode pour veiller à ce que les données de recensement ne soient pas stockées à l'extérieur du ministère.

Nous avons surveillé les préparatifs du recensement en procédant à l'examen des documents et en visitant le Centre de traitement des données (CTD) de Statistique Canada. Nous sommes convaincus que des précautions raisonnables sont prises pour garantir l'intégrité et la confidentialité des données de recensement. Outre les dispositions contractuelles et stratégiques, ces mesures comportent une évaluation indépendante de la sécurité de la TI du Centre, une évaluation des risques et le contrôle de la circulation bidirectionnelle, entre le Centre et l'extérieur. Nous avons attiré l'attention de Statistique Canada sur la nécessité de modifier la documentation sur les procédures afin de préciser que, dans le cadre du recensement de 2006, il n'y aurait pas d'accès à distance au CTD.

Le service en ligne Repérer un colis de Postes Canada

En 2005, nous avons fait enquête sur les lacunes manifestes du service électronique de repérage des colis de la Société canadienne des postes. La Société a accepté d'améliorer plusieurs de ses pratiques, notamment par des procédures d'authentification de l'identité des clients demandant des renseignements, par des moyens d'informer les clients que leur signature se retrouvera prochainement dans Internet, en veillant à ce que leur signature n'apparaisse pas sur le courrier recommandé lorsque les clients s'y opposent et, enfin, par des moyens employés pour rappeler aux clients qu'il est important de protéger leur NAS.

- Conseiller aux institutions de surveiller les programmes d'enregistrement des transactions afin de protéger les renseignements personnels contre l'accès non autorisé

Le Commissariat a remarqué une tendance à l'augmentation des échanges d'information entre les corps policiers et les organismes chargés de la sécurité nationale aux fins de l'application de la loi et de la prévention du terrorisme. Nous pourrions regrouper plusieurs des EFVP examinées dans ces catégories. Nous inquiétons du fait que nous recevons des évaluations présentées sous forme d'éléments projets potentiellement intrusifs, évaluations présentées sous forme d'éléments disjoints plutôt que sous forme d'une analyse exhaustive. Le Commissariat a recommandé à des institutions comme Transports Canada, l'ASFC et la GRC d'élaborer, dès le début de leurs vastes projets intégrés, un cadre de gestion de la protection des renseignements personnels et/ou une EFVP exhaustive.

La tendance des institutions gouvernementales à former des réseaux intégrés pour échanger les renseignements personnels pose de nouveaux défis. Si plusieurs ministères et organismes versent des données à un réseau accessible à des partenaires d'une autre juridiction, surgissent alors des problèmes de gouvernance, de conservation et de contrôle de l'information; des questions se posent alors concernant le consentement et le droit d'accès et de correction.

Le CPVP continuera de surveiller certains des projets de grande envergure par l'examen et la mise à jour des EFVP en s'intéressant notamment au Réseau canadien de l'information sur la sécurité publique (RCISP). Cette initiative, qui relève de Sécurité publique et Protection civile Canada (SPPC), vise à créer un réseau national d'échange d'information à l'intention du système de justice pénale et des organismes chargés de l'application de la loi; il s'agit de relier des sources de données auparavant distinctes concernant la criminalité et les délinquants. Le Commissariat surveillera également les projets entraînant la collecte et l'analyse de renseignements personnels sur les voyageurs obtenus aux postes frontaliers et ou par le biais des systèmes de réservation.

Le Commissariat continuera d'inciter les ministères à se doter d'une structure administrative formelle, sous la forme, par exemple, d'un comité ou d'un groupe de travail interne, qui serait spécifiquement chargé d'examiner les initiatives de l'organisme pour déterminer s'il y a lieu de procéder à une EFVP et d'appliquer les mesures d'atténuation des risques suite à une EFVP. Le CPVP envisage sérieusement de procéder à une vérification du système des EFVP à l'échelle du gouvernement

Par exemple, les EFVP ne mentionnent qu'en termes généraux que le personnel sera informé de ses responsabilités de protéger les renseignements personnels, ou encore, que le personnel sera « avisé » de ses responsabilités. Le Commissariat préfère une méthode plus précise et proactive et il a recommandé la publication de directives et de protocoles exécutaires et de procédures bien étayées.

De même, les EFVP qui nous ont été présentées ne comportent pas nécessairement de procédure permettant aux ministères et organismes d'informer les personnes concernées de situations où leurs renseignements personnels auraient été communiqués contrairement à la loi, accidentellement ou en raison d'un vol. Nous recommandons à tous les ministères de se doter d'une politique claire pour guider les gestionnaires et les employés lorsque des renseignements personnels sont égarés. Voici d'autres exemples de recommandations courantes pour faciliter l'atténuation des risques :

- Demander aux institutions gouvernementales d'intégrer des mesures garantissant la protection de la vie privée aux contrats de traitement ou de stockage de renseignements personnels, notamment sous la forme de vérifications périodiques des pratiques des entrepreneurs
- Recommander qu'une reconnaissance de responsabilité claire concernant la protection des renseignements personnels soit incluse dans les ententes de service
- Veiller à ce que les résumés d'EFVP soient rédigés en termes clairs et non techniques et qu'ils soient affichés sur les sites Web des ministères
- Rappeler aux institutions leur obligation de modifier les banques de données personnelles en fonction des nouveaux renseignements recueillis ou des nouveaux usages prévus de cette information, conformément à la Loi sur la protection des renseignements personnels
- Offrir une formation à tout le personnel en matière de pratiques de protection des renseignements personnels et veiller à ce que toutes les procédures administratives soient conformes aux dispositions de la Loi sur la protection des renseignements personnels

- Un système qui permet aux demandeurs d'assurance-emploi (AE) de remplir et de présenter en ligne les rapports exigés en se servant d'un ordinateur, à la maison ou dans un centre d'emploi
 - Un projet de TPSCG visant à offrir, grâce à des contrats, des services bancaires aux Canadiennes et aux Canadiens qui vivent à l'étranger afin que ces derniers reçoivent rapidement des prestations du gouvernement, par exemple, leur pension de retraite
 - Une étude sur la santé respiratoire des enfants effectuée auprès de 25 000 élèves du primaire
 - Un projet d'identification des voyageurs à risque élevé, qui permettra à l'ASFC de recueillir des renseignements sur les voyageurs aériens à destination des États-Unis et d'échanger ces renseignements avec les États-Unis, ainsi que de recueillir et d'analyser des renseignements personnels sur les voyageurs arrivant par avion au Canada
 - Un projet de vérification pré-embarquement comportant la surveillance vidéo, par l'Administration canadienne de la sûreté du transport aérien (ACSTA), des passagers dans les zones d'embarquement des aéroports, et ce, à l'échelle nationale
 - Un projet des Forces armées canadiennes pour l'enregistrement électronique des dossiers de santé permettant de recueillir des données sur la santé physique, dentaire et psychologique de plus de 80 000 membres du personnel militaire
 - L'usage par Citoyenneté et Immigration Canada d'outils biométriques (empreintes digitales et photos) dans le cadre d'essais expérimentaux aux postes frontaliers et comme mode de vérification des demandeurs d'asile
- Comme nous venons de le voir, les projets examinés sont diversifiés et, dans bien des cas, doivent faire l'objet de recommandations adaptées au type de renseignements recueillis et au type de systèmes employés. Il existe cependant des similitudes dans les types de risques associés à la protection des renseignements personnels et dans les pratiques optimales généralement adoptées pour atténuer les risques.

renseignements personnels. Nous sommes d'avis que cette politique a porté à leur attention des problèmes que pourraient soulever un certain nombre de programmes du gouvernement. Toute cette procédure offre une meilleure garantie de protection des renseignements personnels que les Canadiennes et les Canadiens confient au gouvernement fédéral. Un système d'EFVP efficace est le fondement d'un cadre efficace de gestion de la protection des renseignements personnels.

Nous notons avec satisfaction que plusieurs EFVP que nous recevons sont plus précises et approfondies depuis l'entrée en vigueur de la politique. Il y a cependant encore place à l'amélioration. Par exemple, le Commissariat encourage les ministères à inclure dans leurs présentations le plan d'action pour la mise en œuvre de stratégies de protection des renseignements personnels.

Au cours de cet exercice, le CPVP s'est intéressé à toutes sortes de projets réalisés par un certain nombre de ministères, dont Ressources humaines et Développement des compétences Canada (RHDC), Santé Canada, la Gendarmerie royale du Canada (GRC), Transports Canada, Affaires indiennes et du Nord Canada, Citoyenneté et Immigration Canada, Revenu Canada, l'École de la fonction publique du Canada, Développement social Canada, Anciens combattants Canada, Travaux publics et Services gouvernementaux Canada (TPSGC), Statistique Canada, l'Administration canadienne de la sûreté du transport aérien, l'Agence des services frontaliers du Canada (ASFC), la Défense nationale, Financement agricole Canada et le Centre canadien des armes à feu. Aussi diverses que puissent être les responsabilités de ces ministères, leurs projets ont une caractéristique commune : ils comportent tous la collecte, l'utilisation, la conservation, l'échange ou la transmission de renseignements personnels sur les Canadiennes et les Canadiens.

Les exemples suivants d'EFVP donnent une idée de l'éventail et de l'importance des projets que nous avons examinés :

- L'Outil de recherche intégré de la GRC, application en ligne qui permet de rassembler des données provenant de bases de données policières distinctes en un même dépôt central, offrant la possibilité d'une capacité intégrée de recherche et de constituer un rapport complet sur une personne
- Le projet de renouvellement du Centre d'information de la police canadienne de la GRC et les accords d'échange de renseignements conclus avec d'autres juridictions

Importance des évaluations des facteurs relatifs à la vie privée (EFVP)

Le Commissariat procède à l'examen des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP) effectuées par les institutions gouvernementales au regard de divers projets. Nous recommandons par la suite des moyens de réduire les risques à la protection des renseignements personnels des Canadiennes et des Canadiens.

L'évaluation des facteurs relatifs à la vie privée est un outil permettant de garantir que la protection des renseignements personnels est au cœur des préoccupations dans la planification et l'exécution des projets. Les EFVP servent à décrire et à consigner la nature des renseignements recueillis, leur mode de collecte, d'utilisation, de transmission et de stockage, ainsi que le mode et les raisons de leur échange et le système de protection en place pour prévoir, à chaque étape, la divulgation non prévue des renseignements personnels. En bref, il s'agit d'un outil d'atténuation des risques.

Selon la politique du Secrétaire du Conseil du Trésor (SCT), des EFVP doivent être prévues dans les propositions associées à tous les nouveaux programmes et services soulevant des questions en matière de protection des renseignements personnels et lorsque des programmes en cours sont restructurés de telle sorte que ceux-ci ont une incidence sur la collecte, l'utilisation ou la communication de renseignements personnels – y compris la conversion des services gouvernementaux pour leur usage et leur exécution en ligne.

La politique du SCT, entrée en vigueur en 2002, prévoit également que les institutions fédérales doivent présenter leurs EFVP et leurs EPFVP au Commissariat pour examen. Nous pouvons alors analyser la circulation des données et les mesures prises pour régler les problèmes éventuels. Nous nous assurons qu'il existe une réglementation autorisant la collecte et l'utilisation de renseignements personnels des Canadiennes et Canadiens et que les dispositions et les principes de la *Loi sur la protection des renseignements personnels* sont respectés. Nous signalons aux ministères et organismes les problèmes éventuels qui pourraient avoir échappé à leur attention et, s'il y a lieu, nous formulons des recommandations visant à améliorer la protection des renseignements personnels. Dans certains cas, nous allons jusqu'à demander que des projets soient modifiés de façon significative.

Le CPVP estime que la politique des EFVP a considérablement contribué à la sensibilisation des institutions gouvernementales en matière de protection des

- L'ASFC devrait envisager des moyens d'améliorer la qualité et le contrôle des données qu'elle obtient dans le cadre du Système d'information préalable sur les voyageurs/dossier passager (SIPV/DP) pour s'assurer que les renseignements personnels employés pour remplir le mandat de l'Agence en matière douanière sont aussi exacts et complets que possible.

- L'ASFC n'a pas encore évalué l'efficacité de l'Initiative d'identification des voyageurs à risque élevé (IIVRE) établie avec les États-Unis, car ce projet n'a pas atteint sa pleine mise en œuvre. Elle devrait plus particulièrement évaluer la mesure dans laquelle des renseignements inexacts ou incomplets risquent d'avoir des répercussions sur des personnes ou sur la capacité de l'Agence à identifier, entrer ou appréhender des voyageurs à risque élevé. Une évaluation permettrait à l'Agence de démontrer que l'IIVRE a atteint ses objectifs en matière d'exécution de la loi et du renseignement et, par conséquent, que ses activités de collecte, d'utilisation et d'échange d'innombrables renseignements personnels sur des millions de voyageurs sont justifiées.

- Puisque l'ASFC est un organisme récent, le moment est propice pour qu'elle élabore un cadre exhaustif de gestion de la protection des renseignements personnels et l'intègre à ses activités quotidiennes de gestion de l'information. Elle devrait plus particulièrement s'efforcer de mettre à jour et de consolider les obligations formulées dans ses accords d'échange de renseignements personnels avec les États-Unis. Elle devrait également consolider son système redditionnel concernant les incidents liés à la protection de la vie privée et trouver des moyens de surveiller les communications transfrontalières de renseignements personnels à destination d'organismes chargés de l'application de la loi et autres organismes étrangers.

- Enfin, les activités associées à l'échange transfrontalier de données devraient être aussi transparentes que possible. Nous ne disposons pas d'une description claire et complète de l'information échangée, ni ne savons avec précision avec qui et dans quel but l'information est échangée. À l'instar de la plupart des ministères, l'ASFC ne fournit pas suffisamment de détails sur la circulation transfrontalière de renseignements personnels ni n'en rend compte de façon significative au Parlement et à la population canadienne.

Notre vérification a donné lieu à 19 recommandations à l'intention de l'ASFC (voir le rapport intégral). D'ici deux ans, le CPVP fera un suivi pour évaluer les progrès de l'Agence dans la mise en œuvre de ces recommandations.

Les conclusions formulées dans le rapport de vérification ont pris effet en novembre 2005, c'est-à-dire au moment où l'examen était essentiellement terminé.

Nos principales conclusions

Le CPVP a constaté que l'ASFC est dotée de politiques, de procédures et de systèmes de gestion et d'échange de renseignements personnels avec d'autres pays. Il est cependant possible pour l'Agence d'améliorer considérablement la gestion des risques et de garantir une plus grande responsabilité et un contrôle plus rigoureux des renseignements personnels qui circulent par-delà les frontières canadiennes. Voici les principales conclusions :

- Les demandes écrites adressées par des gouvernements étrangers desirant d'obtenir des documents de l'ASFC sont traitées conformément aux exigences applicables. À l'échelle régionale, toutefois, une large part des échanges de renseignements entre l'ASFC et les États-Unis se fait verbalement, sans demande écrite préalable, ce qui est contraire à la politique de l'Agence et à l'Accord d'assistance mutuelle en matière douanière conclu en juin 1984 entre le Canada et les États-Unis.
- L'ASFC a besoin d'une méthode coordonnée de repérage et de suivi pour tout échange transfrontalier de données. L'Agence ne peut, avec une certitude raisonnable, rendre compte de la mesure dans laquelle elle échange des renseignements personnels avec les États-Unis, de la quantité des renseignements échangés, ni de la fréquence de ces échanges. Par extension, elle ne peut affirmer avec certitude que toutes les activités d'échange de renseignements sont gérées de façon appropriée et se conforment à l'article 107 de la Loi sur les douanes et à l'article 8 de la Loi sur la protection des renseignements personnels.
- En général, les contrôles de TI et de gestion sont valables pour le Système intégré d'exécution des douanes (SIED) et pour le Système d'information sur les passagers (SIPAX). Ces systèmes contiennent des renseignements personnels de nature délicate sur des millions de voyageurs. Les juridictions étrangères, notamment, n'avaient pas directement accès à ces systèmes. Deuxièmement, la communication électronique d'information en direction des États-Unis dans le cadre des initiatives de l'ASFC concernant les voyageurs à risque élevé et l'échange d'avis de surveillance s'effectue par voies sécurisées. Il est cependant possible de consolider les contrôles et de réduire davantage le risque que des renseignements personnels soient utilisés ou communiqués indûment.

faire preuve d'une plus grande transparence pour atténuer les préoccupations de la population canadienne.

La vérification de l'ASFC s'avère une mesure importante, car les Canadiennes et les Canadiens sont préoccupés par la transmission de leurs renseignements personnels aux États-Unis et de la possibilité que leurs renseignements soient employés à des fins autres que la prévention contre le terrorisme et le crime international. La population canadienne, tout comme le Parlement, veut savoir si l'ASFC, l'organisme fédéral le plus directement engagé dans le maintien de la sécurité à la frontière, échange des renseignements personnels avec ses homologues étrangers chargés de l'application de la loi et des activités liées au renseignement et ce, dans le respect des lois sur la protection des renseignements personnels et de façon à préserver le droit à la vie privée des Canadiennes et des Canadiens.

Il est indispensable de compter sur des pratiques solides de reddition de compte et de gestion de la protection de la vie privée pour apaiser les inquiétudes des citoyens concernant la circulation des renseignements personnels entre le Canada et d'autres pays. L'objectif de la vérification était donc de déterminer si l'ASFC contrôle et protège suffisamment les renseignements personnels des Canadiennes et des Canadiens qu'elle transmet à des gouvernements étrangers. Nous nous sommes particulièrement intéressés aux programmes et systèmes associés à la gestion des renseignements personnels des voyageurs. Nous avons examiné les aspects suivants :

1. L'application des mesures douanières et les activités de renseignement (frontière terrestre et aéroports)
2. Le Système intégré d'exécution des douanes (SIED)
3. Le Système d'information sur les passagers (SIPAX)
4. Le Centre national d'évaluation des risques (CNEER)

Le CPVP s'est également intéressé au cadre global de gestion de la protection des renseignements personnels de l'Agence et à la façon dont celle-ci rend compte aux Canadiennes et aux Canadiens des échanges d'information avec d'autres pays.

Nous avons employé les moyens suivants : entrevues avec des employés de l'ASFC, examen de documents (dont les registres d'échanges transfrontaliers de renseignements personnels) et examen des traités, accords, politiques et pratiques relatifs à l'échange d'information entre gouvernements ou organismes gouvernementaux. Un comité externe spécial, créé pour les besoins de la vérification, a été chargé de diriger ces activités.

possibilité d'incliquer plus profondément les principes de gestion de la protection des renseignements personnels en intégrant des exigences d'autoévaluation à cet égard dans les ententes contractuelles avec le gouvernement fédéral. Cette mesure encouragerait fortement les entreprises à se conformer aux principes de protection des données, une responsabilité sociale essentielle pour toute partie qui sous-traite auprès du gouvernement fédéral.

L'importance de la circulation transfrontalière des données est soulignée dans notre vérification de l'Agence des services frontaliers du Canada dont il est également question dans ce chapitre. Cela nous rappelle que la protection des renseignements personnels fait partie intégrante du fonctionnement des ministères et organismes et qu'il ne s'agit pas seulement d'un principe applicable aux contrats conclus avec des tiers. Le CPVP les invite instamment à en faire une meilleure gestion et à en rendre compte plus précisément au Parlement et à la population canadienne.

Le travail du SCT concernant la circulation transfrontalière des données a fait progresser l'élaboration du cadre de gestion de la protection des renseignements personnels. Le Secrétariat prévoit que le cadre comprendra des pratiques optimales, des méthodes et des outils de gestion des risques éprouvés. Il s'agit de veiller à ce que les institutions fédérales respectent des normes strictes de gestion de la protection des renseignements personnels. On nous a laissés entendre que le SCT créerait un comité interministériel de la protection des renseignements personnels qui sera chargé de collaborer à l'élaboration du cadre de gestion de la protection de la vie privée.

Nous continuerons de surveiller l'évolution de la situation et nous examinerons la façon dont les ministères et organismes adaptent les nouvelles instructions relatives aux contrats lorsque nous procéderons à la vérification des entités fédérales assujetties à la Loi sur la protection des renseignements personnels.

Contrôle et responsabilisation accrues en matière de circulation transfrontalière des données

Nous venons de terminer une vérification d'envergure de l'Agence des services frontaliers du Canada (ASFC). Voici un résumé des résultats de la vérification (le rapport complet se trouve sur le site Web du Commissariat : www.privcom.gc.ca). La vérification de l'Agence et l'examen des renseignements publics sur la circulation transfrontalière des données nous amène à conclure que, dans l'ensemble, un contrôle et une responsabilisation accrues sont nécessaires. Le gouvernement devrait

- Élaborer d'autres lignes directrices concernant l'échange d'information entre gouvernements (au Canada et à l'étranger), la vérification des contrats et les solutions techniques permettant de protéger les renseignements personnels Augmenter la sensibilisation et la formation au sujet de la circulation transfrontalière des données et sur les mesures de sécurité fédérales qui ont cours
- Procéder à l'examen de la *LPRPD* en 2006 et déterminer si la *Loi sur la protection des renseignements personnels* doit également faire l'objet d'un examen (le CPVP estime que cela devrait être fait depuis longtemps)
- Examiner les questions relatives à la protection des renseignements personnels et de la circulation transfrontalière des données dans le cadre du futur Partenariat pour la sécurité et la prospérité entre le Canada, les États-Unis et le Mexique
- Mettre en commun les pratiques optimales de protection de la circulation transfrontalière des données avec les gouvernements provinciaux et territoriaux ainsi qu'avec le secteur privé et les gouvernements étrangers

Nous félicitons également le SCT pour ses récents efforts en vue d'élaborer une liste de contrôles visant la protection de la vie privée, c'est-à-dire une série de principes et de questions permettant aux institutions gouvernementales de rédiger des clauses contractuelles valables en matière d'accès à l'information et de protection des renseignements personnels.

Lorsqu'elle conclut un contrat de service, la direction d'un programme ou d'un service gouvernemental doit s'assurer que le contrat ne mine pas le droit d'accès à l'information ou qu'il ne met pas considérablement à risque la capacité du ministère de protéger les renseignements personnels des individus. Cette responsabilité demeure inchangée lorsque les ministères ont recours à l'impartition. L'un des moyens d'exiger qu'un fournisseur de services extérieur respecte les dispositions de la *Loi sur la protection des renseignements personnels* est d'insérer dans le contrat, s'il y a lieu, les clauses qui conviennent. Ainsi, le contrat contribue à garantir que la responsabilité de l'institution gouvernementale en matière de protection des renseignements personnels est assumée par l'entrepreneur.

En mars 2006, le CPVP a proposé au SCT d'apporter d'autres améliorations à la procédure d'attribution des contrats du gouvernement en envisageant l'instauration de mesures permettant aux entreprises de rendre compte de leur capacité de gestion de la protection des renseignements personnels lorsque celles-ci désirent être admissibles aux contrats du gouvernement fédéral. Nous y voyons la

L'intention des institutions fédérales, les invitant à tenir compte de la protection des renseignements personnels avant de conclure des contrats. Ces documents peuvent être consultés sur le site Web du SCT (www.tbs-sct.gc.ca). Voici quelques-unes des mesures prises par le gouvernement :

- L'ensemble des 160 institutions gouvernementales assujetties à la *Loi sur la protection des renseignements personnels* ont été sensibilisées aux problèmes en matière de protection des renseignements personnels découlant de la *USA PATRIOT Act*.
- Les institutions ont été invitées à réexaminer leurs contrats et leurs modalités d'impartition pour circonscrire les risques associés à l'application de la *USA PATRIOT Act*, déterminer la gravité de ces risques, prendre les mesures correctives en conséquence et en rendre compte au SCT. Selon les résultats obtenus, 83 % des institutions considèrent que leurs contrats ne comportent pas de risques (77 institutions) ou comportent un faible risque (57 institutions).

- Le gouvernement a fait la promotion de pratiques optimales dans le cadre des modalités d'impartition; les institutions fédérales disposent d'un guide stratégique, qui comprend une liste de contrôles, des conseils directs sur l'importance de l'examen des questions associées à la protection des renseignements personnels avant de passer des contrats, des moyens de maximiser la protection des renseignements personnels et de l'aide pour la rédaction de clauses pouvant être incluses dans les demandes de propositions et appels d'offres.

La stratégie fédérale prévoit d'autres mesures pour atténuer les risques en matière de protection des renseignements personnels. Certaines sont énumérées ci-dessous; elles illustrent le travail considérable que suppose le règlement de cette question.

- Elaborer un cadre de gestion de la protection de la vie privée pour instaurer des normes de protection élevées dans l'ensemble de la fonction publique fédérale
- Procéder à l'évaluation continue des activités contractuelles des entités fédérales et fournir des conseils concernant les contrats (SCT)
- Explorer les solutions offertes par la technologie et l'architecture des données pour protéger la circulation de données et, notamment l'usage de techniques de chiffrement et de pistes de vérification électronique

Nécessité d'un cadre de gestion de la protection de la vie privée plus rigoureux

L'an dernier, le Commissariat a fait part de la nécessité d'établir un cadre de gestion de la protection de la vie privée pour le gouvernement fédéral. Nous avons précisé ce qu'est un cadre de gestion, en quoi il est important, et nous avons décrit les caractéristiques d'un cadre adéquat de protection de la vie privée. Nous avons également fait des observations sur certains enjeux à aborder en vue de renforcer la gestion de la protection de la vie privée au sein du gouvernement fédéral.

Le Secrétaire du Conseil du Trésor du Canada (STC) a pour responsabilité d'établir les orientations politiques en matière de protection de la vie privée et de fournir de l'encadrement aux institutions fédérales. L'an dernier, le Commissariat a recommandé au SCT d'élaborer un modèle de cadre pour orienter la gestion de la protection de la vie privée dans les ministères et organismes fédéraux. La direction du SCT a accepté cette recommandation, indiquant qu'elle s'était engagée à mettre de l'avant le concept du cadre proposé et qu'elle examinerait la portée et le processus d'un tel projet.

Bien que le Commissariat remarque le progrès effectué en ce sens, toutes les parties reconnaissent qu'il reste encore beaucoup à faire.

En décembre 2005, le SCT nous a informés que des fonctionnaires avaient commencé à examiner les concepts préliminaires éayant la conception et l'élaboration d'un cadre de gestion de la protection de la vie privée pour énoncer la vision et la stratégie du gouvernement en la matière. Ce cadre sous-tendra une infrastructure complète de gestion et de responsabilisation axée sur les risques en matière de protection des renseignements personnels afin de garantir l'équilibre qui convient entre le droit à la vie privée des Canadiennes et des Canadiens et d'autres objectifs et mandats associés à l'intérêt public et aux programmes du gouvernement. Un projet était déjà en cours de réalisation pour consolider et mettre à jour diverses politiques portant sur les évaluations des facteurs relatifs à la vie privée, le couplage de données, la protection des données et l'usage du NAS – soit des enjeux qui intéressent le CPVP.

Le SCT a consulté le CPVP lors de l'élaboration d'une stratégie fédérale en réponse aux préoccupations suscitées par la *USA PATRIOT Act* et la circulation transfrontalière de données (voir plus haut). Le gouvernement a bien réagi face à cet enjeu. À la fin de mars 2006, le SCT a publié sa stratégie et des lignes directrices à

L'incombe au Commissariat à la protection de la vie privée du Canada d'effectuer la vérification des ministères et organismes fédéraux assujettis à la *Loi sur la protection des renseignements personnels*. Il peut également effectuer des vérifications d'organisations du secteur privé en vertu du paragraphe 18(1) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Le Commissariat examine également les évaluations des facteurs relatifs à la vie privée (EFVP) préparées par les ministères ou organismes fédéraux. Il réalise en outre divers autres projets relatifs aux pratiques en matière de protection de la vie privée dans les secteurs public et privé.

Grâce à la fonction de vérification et d'examen, le Commissariat peut assumer son rôle de défenseur du droit à protection de la vie privée. Cette fonction consiste à mener, de manière indépendante et objective, des vérifications et des examens de systèmes de gestion des renseignements personnels afin de promouvoir la conformité aux lois, aux politiques et aux normes, mais aussi afin d'améliorer les pratiques en matière de protection de la vie privée et de reddition de comptes.

Au cours de l'exercice 2005-2006, le Commissariat a mené à terme une vérification majeure effectuée en vertu de la *Loi sur la protection des renseignements personnels*; il a complété l'essentiel de trois autres projets de vérification et entrepris un examen des entités fédérales non assujetties à la *Loi sur la protection des renseignements personnels* ou à la LPRPDE. Il a également effectué 43 examens d'évaluation des facteurs relatifs à la vie privée et 16 autres projets. Le personnel du Commissariat a également assuré la surveillance des activités relatives à la protection de la vie privée du Secrétariat du Conseil du Trésor et d'autres ministères et organismes fédéraux.

Statistiques sur les demandes de renseignements
1^{er} avril 2005 au 31 mars 2006

Demandes de renseignements en vertu de la Loi sur la protection des renseignements personnels reçues par la Direction des enquêtes et des demandes de renseignements		
Demandes téléphoniques	1 929	
Demandes écrites (lettres, courriels, télécopies)	577	
Nombre total de demandes de renseignements reçues	2 506	
Demandes de renseignements en vertu de la Loi sur la protection des renseignements personnels fermées par la Direction des enquêtes et des demandes de renseignements		
Demandes téléphoniques	1 933	
Demandes écrites (lettres, courriels, télécopies)	631	
Nombre total de demandes réglées	2 564	

La Direction des enquêtes et des demandes de renseignements répond aux demandes de renseignements du grand public au sujet de l'application de la Loi sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE). Le Commissariat reçoit chaque année des milliers de demandes de renseignements du public et d'organisations qui veulent obtenir des conseils sur des enjeux concernant la protection des renseignements personnels dans le secteur privé.

Au cours de l'exercice financier 2005-2006, le Commissariat a reçu 2 506 demandes de renseignements concernant la Loi sur la protection des renseignements personnels, soit un peu moins que les 2 976 demandes de renseignements reçues l'année précédente. En comparaison, nous avons reçu plus que le double du nombre de demandes de renseignements sur des questions touchant la LPRPDE (voir les statistiques dans notre rapport annuel 2005 sur la LPRPDE présenté au Parlement).

Le personnel responsable des demandes de renseignements répond peut-être à moins d'appels, mais il fournit plus d'information. Par suite de la décision prise en 2004 de ne plus accepter les demandes de renseignements par courriel, nous avons procédé à une restructuration du temps consacré par le personnel aux demandes de renseignements téléphoniques. Les personnes qui appellent demandent en général des explications plus longues et plus détaillées en réponse à leurs questions. En outre, un système téléphonique automatisé répond aux questions les plus fréquemment posées par le grand public, comme celles sur le vol d'identité, le télémarketing et le numéro d'assurance sociale. Notre site Web renferme également une vaste gamme de renseignements.

Sur l'ensemble des demandes de renseignements présentées en vertu de la Loi sur la protection des renseignements personnels, environ 25 % sont émises par écrit et 75 % par téléphone. En moyenne, nous répondons aux demandes de renseignements formulées par écrit dans un délai de trois mois. La majorité des personnes qui demandent des renseignements par téléphone reçoivent une réponse immédiate. Les autres, pour lesquelles nous devons mener certaines recherches, reçoivent une réponse dans les trois jours suivant leur appel.

Analyse :

L'enquêteur analyse les faits et prépare les recommandations pour la commissaire à la protection de la vie privée ou sa déléguée. L'enquêteur communique avec les parties et examine les faits recueillis au cours de l'enquête. Il informe également les parties des recommandations, fondées sur les faits, qu'il présentera à la commissaire à la protection de la vie privée ou sa déléguée. À cette étape, les parties peuvent formuler d'autres observations.

Au besoin, des consultations internes sont effectuées avec, par exemple, le concours de la Division des services juridiques ou de la Direction de la recherche et des politiques.

Conclusion :

La commissaire à la protection de la vie privée ou sa déléguée examine le dossier, évalue le rapport et prend une décision au sujet de la recommandation. La commissaire ou sa déléguée, et non l'enquêteur, décide de l'issue appropriée du dossier et s'il faut présenter des recommandations à l'institution.

La commissaire à la protection de la vie privée ou sa déléguée envoie une lettre expliquant ses conclusions aux parties. Cette lettre présente le fondement de la plainte, les faits établis, l'analyse effectuée par la commissaire ou sa déléguée, ainsi que toute recommandation faite à l'institution. La commissaire à la protection de la vie privée ou sa déléguée peut demander à l'institution de lui indiquer par écrit, dans un délai précis, les mesures prévues pour mettre en œuvre les recommandations.

Les conclusions possibles sont les suivantes :

Non fondée : La preuve ne permet pas à la commissaire à la protection de la vie privée ou sa déléguée de conclure que les droits du plaignant en vertu de la Loi ont été enfreints.

Fondée : L'institution n'a pas respecté l'une des dispositions de la Loi.

Fondée et résolue : L'enquête permet de justifier les allégations, et l'institution s'engage à prendre des mesures correctives pour remédier au problème.

Résolue : La preuve recueillie au cours de l'enquête soutient les allégations soulevées dans la plainte, mais l'institution s'engage à prendre des mesures pour corriger le problème; le Commissariat juge les mesures appropriées. Cette conclusion est tirée dans les situations où, compte tenu que la plainte découle principalement d'un problème de communication, il serait trop sévère de conclure qu'elle est fondée. Dans la lettre de conclusions, la commissaire à la protection de la vie privée ou sa déléguée informe le plaignant de son droit de recours à la Cour fédérale pour les cas de refus d'accès aux renseignements personnels.

Lorsque des recommandations sont présentées à une institution, le personnel du CPVP effectue un suivi pour vérifier si elles ont bel et bien été appliquées.

Lorsqu'on lui refuse l'accès à ses renseignements personnels, le plaignant, ou la commissaire à la protection de la vie privée, peut choisir de demander une audience à la Cour fédérale. La Cour fédérale a le pouvoir d'examiner l'affaire et de déterminer si l'institution doit fournir les renseignements au requérant.

Résolue?

Le CPVP cherche à régler les plaintes et à prévenir d'autres infractions à la Loi. La commissaire favorise la résolution des différends par l'entremise de la médiation, de la négociation et de discussions persuasives. L'enquêteur participe au processus.

Note : une ligne discontinue (---) indique un résultat possible.

Processus d'enquête en vertu de la Loi sur la protection des renseignements personnels

Demande de renseignements : Une personne communique avec le CPVP par lettre, par téléphone ou en personne pour déposer une plainte relative à une infraction à la loi. Les personnes qui communiquent par téléphone ou en personne doivent par la suite présenter leurs allégations par écrit.

Analyse initiale :

Le personnel des enquêtes examine l'affaire en cause afin de déterminer si elle constitue bel et bien une plainte, c'est-à-dire de déterminer si les allégations, dans l'éventualité où elles s'avèrent fondées, peuvent contrevenir à la loi.

Une personne peut déposer une plainte à toute question énoncée à l'article 29 de la Loi sur la protection des renseignements personnels – par exemple, le refus d'une institution de communiquer à une personne les renseignements personnels qu'elle détient à son sujet, ou un retard inacceptable dans la communication de ces renseignements; la collecte, l'utilisation ou la communication inappropriée de renseignements personnels; des erreurs dans les renseignements personnels qu'une institution utilise ou communique.

Plainte?

Non :

La personne est informée, par exemple, que la question ne relève pas de notre organisme.

Oui :

Un enquêteur est affecté au dossier.

Enquête :

L'enquête permet d'établir les faits sur lesquels la commissaire s'appuie pour déterminer si les droits des personnes garantis par la Loi sur la protection des renseignements personnels ont été enfreints.

L'enquêteur explique à l'institution, par écrit, l'essentiel de la plainte. Il rassemble les faits se rapportant à la plainte en recevant les observations des deux parties, ainsi que par une enquête indépendante, des entrevues avec les témoins et l'examen de la documentation. Au nom de la commissaire à la protection de la vie privée, l'enquêteur a le pouvoir de recevoir des éléments de preuve, d'accéder à des lieux au besoin et d'obtenir ou d'examiner des copies de dossiers trouvés sur place.

Analyse (suite)

Résolue? (suite)

Abandonnée? Une plainte peut être abandonnée si, par exemple, un plaignant décide de ne pas continuer avec sa plainte, ou s'il ne peut être localisé.

Règlement rapide? Une plainte peut être résolue avant qu'une enquête n'ait commencé si, par exemple, la question a déjà été traitée dans le cadre d'une autre plainte et que l'institution a cessé la pratique, ou si cette pratique ne contrevient pas à la loi.

Note : une ligne discontinue (---) indique un résultat possible.

danger pour la collectivité. Nous avons reçu 17 avis de ce genre, dont la majorité provenaient de la Gendarmerie royale du Canada et du Service correctionnel du Canada (SCC).

Le deuxième groupe en importance est constitué des 13 avis provenant du SCC, de la Défense nationale et de la Commission nationale des libérations conditionnelles. Ces avis concernaient la communication de renseignements personnels à des membres de la famille de personnes récemment décédées afin de les informer des circonstances du décès et de les aider à faire leur deuil.

Sept autres avis concernaient la responsabilité gouvernementale à l'égard de questions comme l'enquête d'ippervash relative à l'assassinat de Dudley George, et la Commission d'enquête chargée d'examiner l'incendie à bord du HMCS Chicoutimi.

Notons également six autres avis sur des questions de santé, dont un provenait de Sécurité publique et Protection civile Canada, l'autre du ministère des Affaires étrangères et du Commerce international (MABCI), au sujet des risques à la santé des citoyens que pouvaient présenter des personnes atteintes de tuberculose.

Plusieurs autres avis ont également été émis, dont un du SCC renfermant des renseignements au sujet de la remise en liberté de Karla Homolka, à l'intention de l'avocat de ses victimes.

Au cours de son enquête, le MDN a découvert que l'information était au départ inscrite sur un disque protégé avec accès partagé mais contrôle, restreint aux personnes qui avaient besoin de cette information pour faire leur travail. À un moment donné, les serveurs ont été fusionnés, éliminant ainsi la protection anti-intrusion et rendant l'information disponible sur un disque partagé pendant un certain temps. C'est ainsi que l'employé a pu découvrir la liste.

Une fois avisé du problème, le MDN a immédiatement adopté des mesures pour retirer et détruire la liste. La liste de griefs a depuis été modifiée de façon à ce que l'identité des personnes qui déposent un grief ne soit plus révélée. Le MDN a rappelé aux employés responsables de la liste qu'il est impératif de protéger les renseignements personnels. Il a également écrit à l'employé pour lui expliquer la situation qui avait mené à l'accessibilité de ses renseignements sur un réseau partagé. Le MDN l'a également avisé de son droit de déposer une plainte officielle auprès du Commissariat.

Communications d'intérêt public en vertu de la Loi sur la protection des renseignements personnels

Les chefs des institutions gouvernementales disposent du pouvoir discrétionnaire de communiquer des renseignements personnels sans obtenir le consentement de la personne concernée lorsque la communication est à l'avantage de cette dernière, ou lorsque l'intérêt public prime sur la protection de la vie privée de la personne. Le chef de l'institution doit en aviser la commissaire à la protection de la vie privée au préalable, sauf en cas d'urgence. Le Commissariat examine les communications proposées et, s'il est jugé nécessaire de le faire, la commissaire à la protection de la vie privée avise la personne concernée par l'information. Le Commissariat avise également les institutions lorsqu'il estime que la quantité de renseignements personnels que l'on propose de communiquer excède ce qui satisfait aux questions d'intérêt public. Nous recommandons alors des mesures visant à réduire au minimum l'imixtion dans la vie privée de la personne. Nous avons traité plus tôt dans ce rapport des enjeux concernant cette disposition de la Loi sur la protection des renseignements personnels.

Nous avons effectué l'examen de 66 de ces avis, dont un grand nombre étaient classés dans deux catégories. La première concerne les personnes qui étaient illégalement en liberté, soit remises en liberté à la fin de leur peine. Toutes étaient considérées comme présentant un risque élevé de récidive et, par conséquent, un

Mallette et sac à dos contenant de l'information sur des détenus volés dans le coffre d'une voiture

À l'hiver 2005, deux employés du Service correctionnel Canada (SCC) ont déposé une mallette fermée à clé et un sac à dos dans le coffre de leur voiture personnelle après avoir assisté à une réunion. Arrivés à la maison, ils n'ont pas retiré les articles du coffre. Deux jours plus tard, un des employés a garé le véhicule dans le stationnement d'un centre commercial, pour découvrir à son retour que sa voiture avait été vandalisée. Le lendemain, en vérifiant le contenu du coffre, les deux employés ont constaté que la mallette et le sac à dos avaient disparu. Ils ont immédiatement avisé la GRC et leur employeur. La GRC n'a pas mené d'enquête car le SCC devait effectuer la sienne.

Parmi les documents manquants se trouvait un rapport contenant de l'information sur huit détenus sous responsabilité fédérale. Le SCC a informé seulement deux d'entre eux de l'incident, car les autres étaient décédés. Les auteurs de l'examen effectuée par le SCC en sont venus à la conclusion qu'il n'était pas approprié de transporter de l'information protégée dans un sac à dos et que ni le coffre d'une voiture ni une mallette ne sont des dispositifs approuvés pour entreposer de l'information protégée. Une mallette peut être utilisée pour transporter de tels renseignements; néanmoins, les employés responsables de la protection de l'information auraient dû retirer la mallette du véhicule en arrivant à destination. Par suite de cet incident, le SCC a décidé d'établir des lignes directrices plus précises concernant le transport et la garde des renseignements en dehors des bureaux du SCC.

Un employé du ministère de la Défense nationale (MDN) trouve des renseignements concernant les griefs à son intention sur un disque informatique partagé

Plusieurs incidents sont survenus concernant des disques informatiques partagés, rendant des renseignements personnels accessibles à des personnes qui n'étaient pas autorisées à en prendre connaissance. Dans l'un de ces cas, un employé du MDN a découvert un tableau de griefs sur un disque partagé. Sur ce tableau de griefs se trouvaient listés son nom, le numéro de dossier assigné à sa plainte formulée suite au grief, et l'état relatif au traitement du grief. La liste comprenait des renseignements semblables sur d'autres personnes ayant également déposé des griefs.

- U.S. Department of Defense Standard 5220.22-M – *Advising Users on Computer Systems Technology*, que l'on peut consulter en ligne à l'adresse suivante : http://www.gsgi.com/usdod_standard_dod_522022m.htm

Même si ces documents ne donnent pas de directives précises sur la destruction des rouleaux de papier thermique, les techniques générales qui y sont décrites (p. ex., le déchiquetage) devraient être facilement adaptables.

Vol d'un ordinateur contenant des renseignements sur les laissez-passer de sécurité pour les festivals de la CCN

Au printemps de 2004, un ordinateur portable et ses accessoires ont été volés dans un local de la Commission de la capitale nationale (CCN). Le portable contenait des renseignements personnels provenant de deux banques de données sur la sécurité pour des laissez-passer donnant accès aux divers festivals de la CCN. L'information, incluant noms, photos, dates de naissance, professions et noms de l'employeur, était protégée par deux niveaux de mots de passe.

L'enquête interne de la CCN a révélé qu'on avait procédé à d'importants travaux de construction dans l'immeuble en question au moment où le portable a été volé. Un plus grand nombre de personnes qu'en temps normal avaient accès à l'immeuble où se trouvait l'ordinateur, et il était donc difficile de déterminer qui aurait pu le prendre. La CCN a décidé d'accroître le niveau de sécurité dans cet immeuble. Le Commissariat a confirmé que la CCN avait également fait parvenir des lettres aux employés dont l'information avait été compromise, les dirigeant vers divers sites Web, dont le nôtre, pour trouver de l'information sur la protection contre le vol d'identité. On les a également dirigés vers le Bureau de l'accès à l'information et de la protection des renseignements personnels de la CCN pour y obtenir d'autres conseils. En outre, le Commissariat a recommandé à la CCN de faire une copie d'archive de cette banque d'information afin de prévenir toute perte future en cas de vol ou de destruction d'équipement.

Les fonctionnaires ont accepté d'effectuer un inventaire complet et une remise en état de tous les télécopieurs. Ils ont également communiqué avec le Centre de distribution des biens de la Couronne afin de récupérer tous les appareils semblables non vendus et vérifier si ces derniers renfermaient des renseignements personnels. Le Commissariat est convaincu que toutes les mesures appropriées ont été prises pour remédier à la situation et empêcher que cette situation ne se reproduise.

Cependant, en cours d'enquête, nous avons découvert que deux télécopieurs contenant des rouleaux ThermoFax intacts provenant de l'Agence du revenu du Canada (ARC) avaient également été vendus par le Centre de distribution des biens de la Couronne. Là encore, le personnel n'était tout simplement pas au courant de la nécessité d'épurer les appareils. L'ARC a également modifié ses politiques et procédures concernant la liquidation de matériel contenant de la mémoire.

Compte tenu des vastes répercussions de cette affaire et de la probabilité que tous les ministères et organismes utilisent de l'équipement contenant une mémoire qui doit être éliminée, le Commissariat a mis au fait de cette situation la Direction des politiques de l'information, de la protection des renseignements personnels et de la sécurité du Secrétariat du Conseil du Trésor. Ce dernier examine actuellement la question et publiera un bulletin destiné à tous les ministères et organismes gouvernementaux.

En conclusion, cette situation souligne l'importance d'assurer la destruction de tous les renseignements personnels contenus dans les dispositifs électroniques de stockage de données que possèdent les institutions. La solution ne couvre peut-être pas tous les cas, mais il existe trois façons d'« épurer les appareils » ou de détruire les données électroniques :

- **L'effacement** – entrer les chiffres 1 et 0 par-dessus les données.
- **La démagnétisation** – effacer magnétiquement les données à l'aide d'un démagnétiseur électrique.
- **La destruction** – destruction physique du dispositif de stockage.

Deux documents techniques renferment des conseils sur ces questions :

- Centre de la sécurité des communications – *Effacement et déclassification des supports d'information électronique*, que l'on peut consulter en ligne à l'adresse suivante : <http://www.csc-cst.gc.ca/documents/publications/gov-pubs/litsg/litsg06.pdf>

Incidents en vertu de la Loi sur la protection des renseignements personnels

Outre les plaintes individuelles, le Commissariat fait enquête sur des incidents relatifs à une mauvaise gestion des renseignements personnels. Diverses sources, dont les médias, portent ces incidents à notre attention, ou alors les institutions elles-mêmes nous les signalent directement. Les incidents portent notamment sur la collecte, l'utilisation et la communication inadéquates de renseignements personnels. Ils soulèvent souvent un problème systémique ou une violation jusque-là inconnue de la protection la vie privée qui doit être corrigée dans les meilleurs délais. L'an dernier, le Commissariat a mené à terme 54 enquêtes de ce genre.

On nous a signalé plusieurs incidents relatifs au vol d'ordinateurs ou de mallettes, trois incidents portant sur des renseignements emmagasinés sur des disques informatiques partagés, et deux incidents de vente de télécopieurs dont la mémoire contenait des renseignements personnels. On trouvera une description de ces cas ci-dessous.

Le Centre de distribution des biens de la Couronne vend des rouleaux de papier Thermofax pour télécopieurs contenant des renseignements personnels

Quelques incidents d'achat, après du Centre de distribution des biens de la Couronne, de télécopieurs munis de rouleaux Thermofax contenant des renseignements personnels ont été signalés. Par exemple, en 2005, Ressources humaines et Développement des compétences Canada (RHDC) a informé le Commissariat qu'un représentant des médias avait obtenu un rouleau de papier Thermofax contenant le nom et le numéro d'assurance sociale de 65 personnes. Un rouleau de papier thermique est vendu dans une cartouche qui est chargée dans le télécopieur. Il contient du papier fin ainsi qu'une substance qui s'apparente à un film clair. Lorsque tout le papier de la cartouche a été utilisé, celle-ci doit être remplacée; le film utilisé renferme le négatif de toutes les télécopies reçues par le biais de cet appareil, depuis l'installation du rouleau jusqu'à son retrait. Le rouleau de papier thermique se trouvait dans un télécopieur vendu par le Centre de distribution des biens de la Couronne. Une personne l'a ensuite achetée, puis l'a transmis aux médias. Après enquête de RHDC, l'acheteur a affirmé aux fonctionnaires qu'il avait détruit le rouleau de papier thermique et tous les dossiers qui en avaient été extraits.

RHDC a adopté plusieurs mesures pour s'assurer que ce genre de situation ne se reproduise pas. Une politique modifiée, laquelle vise RHDC, Développement social Canada et Service Canada, insiste sur la nécessité de vérifier l'équipement excédentaire et d'enlever et de détruire comme il se doit la « mémoire » des appareils.

Le gouvernement a le droit de surveiller l'utilisation de ses systèmes de courrier électronique

Un employé de l'Agence des services frontaliers du Canada (ASFC) est contrarié par l'obligation d'acquiescer à un avis s'affichant à son écran d'ordinateur chaque fois qu'il souhaite accéder au système informatique de l'ASFC, sous peine de s'en voir refuser l'accès. L'avis en question indique que l'ASFC peut surveiller l'utilisation de ses systèmes. Selon le plaignant, les principes de protection de la vie privée qui s'appliquent à l'utilisation du téléphone devraient également s'appliquer à l'utilisation du courriel. Il est d'avis que la surveillance de ses courriels constitue une atteinte à son droit à la vie privée.

Le Commissariat a établi que la politique de surveillance de l'ASFC est fondée sur deux politiques du Conseil du Trésor, soit la Politique du gouvernement sur la sécurité et la Politique d'utilisation des réseaux électroniques. Ces politiques établissent clairement que les ministères doivent effectuer une surveillance active et des vérifications internes de leurs programmes de sécurité. Ainsi, les réseaux électroniques peuvent être surveillés pour des raisons opérationnelles et pour évaluer le respect des politiques. Pour la réalisation des analyses de routine, il n'y a aucune lecture de contenu. Néanmoins, si une analyse de routine ou une plainte fournit des motifs raisonnables de croire qu'une personne utilise indûment le réseau, l'affaire fait l'objet d'une enquête, et il peut s'ensuivre des mesures de surveillance spéciales et/ou la lecture du contenu des courriels. Dans le cas qui nous occupe, l'ASFC a affirmé que les courriels personnels du plaignant n'ont jamais été lus.

L'ASFC a souligné que les courriels constituent un outil de communication organisationnel fourni aux employés aux fins d'activités gouvernementales officielles. L'Agence autorise l'utilisation du système de courriels à des fins personnelles, mais de façon restreinte et à condition que les politiques et dispositions légales applicables à l'Agence soient respectées et que le rendement de l'employé n'en souffre pas.

Le Commissariat a conclu que l'ASFC faisait preuve d'équité et de transparence en informant ses employés de ses pratiques de surveillance par le biais de l'avis électronique et en versant à son site intranet les directives s'appliquant à son réseau électronique. Par conséquent, les employés sont parfaitement en mesure d'évaluer le niveau de protection de leur vie privée au sein de l'ASFC. Le Commissariat a jugé que la plainte était non fondée.

L'ARC s'est simplement identifiée comme telle, puis a demandé à obtenir des renseignements pour pouvoir joindre la plaignante. Par conséquent, le Commissariat juge la plainte non fondée.

La Commission de la fonction publique communique des renseignements personnels dans le cadre d'une vérification

Trois personnes ont déposé une plainte selon laquelle la Commission de la fonction publique (CFP) a communiqué de l'information à leur sujet dans le cadre d'une vérification rendue publique.

La CFP a effectué une vérification des mesures de dotation d'un organisme gouvernemental de petite taille. Dans son rapport de conclusions, la Commission donne des exemples de mesures de dotation bien définies visées par sa vérification. Le Commissariat a conclu que même si le rapport ne contenait aucun nom, l'information était suffisamment détaillée pour que des personnes puissent être identifiées. En outre, puisque la vérification a été rendue publique, les conclusions ont également été rapportées par les médias.

Les vérifications soulèvent rarement des aspects positifs; il n'est pas rare que les exemples donnés à l'appui d'une vérification présentent des situations sous un angle péjoratif. Ce n'est pas problématique en soi si une vérification porte sur les processus de dotation d'institutions fédérales qui emploient des centaines de personnes pour différentes classifications d'emploi. Cependant, lorsqu'un organisme de petite taille est visé, les conséquences diffèrent : remettre en question le processus de sélection pour un poste lorsqu'un candidat est identifiable a des répercussions directes sur la perception des compétences et des qualifications de cette personne.

Le Commissariat a conclu que l'information divulguée suite à la vérification de la CFP constitue clairement des renseignements personnels et que le consentement des personnes concernées aurait dû être obtenu avant que l'information ne soit communiquée. Les plaintes sont donc jugées fondées.

À la satisfaction du Commissariat, la CFP exige désormais que les vérifications soient examinées par son équipe responsable de l'accès à l'information et de la protection de la vie privée avant toute communication afin de déterminer si elles contiennent de l'information visée par la Loi sur la protection des renseignements personnels.

plainte relative aux droits de la personne, le Commissariat a conclu que le droit à la protection de la vie privée de la plaignante n'avait pas été bafoué. La plainte est jugée non fondée.

Une débitrice allègue qu'une agente de recouvrement a communiqué ses renseignements personnels

Une personne a déposé une plainte selon laquelle une agente de recouvrement de l'Agence du revenu du Canada (ARC) a communiqué de façon indue ses renseignements personnels à une autre personne.

Le Commissariat a appris que la plaignante devait de l'argent à l'ARC en raison d'un versement excédentaire qu'elle avait obtenu dans le cadre de la prestation fiscale canadienne pour enfants. Elle y était admissible alors qu'elle était mariée, mais a continué à obtenir des versements suite à son divorce, malgré qu'elle n'avait pas la garde de ses enfants. L'ARC a découvert l'erreur lorsque l'ex-mari de la plaignante, ainsi que la mère de celui-ci qui avait alors la garde des enfants, ont fait une demande de prestation fiscale. L'ARC a récupéré une partie des paiements en trop, mais, au bout d'un certain temps, ses lettres de demandes de paiement lui sont revenues, non décachées.

Une agente de recouvrement de l'ARC a été chargée du dossier et a téléphoné à l'ancienne belle-mère de la plaignante, dont le nom figurait aux dossiers de l'ARC à titre de prestataire actuelle. L'agente de recouvrement a fait savoir au Commissariat qu'elle s'était identifiée auprès de la belle-mère avant de préciser qu'elle cherchait à obtenir les nouvelles coordonnées de la plaignante. Cette dernière a affirmé que l'agente de recouvrement a alors communiqué ses renseignements fiscaux personnels relatifs aux prestations. Toutefois, l'agente et la belle-mère ont nié cette affirmation. Elles affirment toutes deux que la belle-mère a immédiatement déduit les raisons pour lesquelles l'agente tentait de joindre sa belle-fille, et que lorsque la belle-mère a interrogé l'agente à ce sujet, celle-ci lui a répondu qu'elle ne pouvait pas divulguer d'information.

En vertu de la *Loi sur l'impôt sur le revenu*, la responsabilité de percevoir les impôts payables au gouvernement du Canada a été déléguée aux agents de recouvrement de l'ARC. Dans la présente situation, les faits démontrent que l'agente de recouvrement de l'ARC n'a fourni à la belle-mère aucun détail sur la plaignante ou sur son dossier fiscal. À notre avis, l'agente de recouvrement a respecté les principes fondamentaux d'équité procédurale applicables aux enquêtes. L'agente de recouvrement de

Au cours de notre enquête, le MDN a indiqué qu'il n'était pas nécessaire, aux fins de son programme d'aide aux familles, d'obtenir le numéro d'assurance sociale du gardien ou de la gardienne d'enfants. Il a donc accepté de modifier son formulaire en conséquence et a avisé ses employés de ne plus demander le numéro d'assurance sociale de leur gardien(ne). Le Ministère a également affirmé que le père en question n'avait pas inscrit le numéro d'assurance sociale de la plaignante dans le formulaire. La plaignante étant satisfaite de l'issue de la plainte, celle-ci est considérée réglée.

Une enquête effectuée par suite d'une plainte relative aux droits de la personne mène à la communication de renseignements sur un employé

Une employée de la Société canadienne des postes (SCP) a déposé une plainte selon laquelle son employeur avait informé un autre organisme de son congé d'invalidité.

Le Commissariat a appris que l'employée de la SCP avait déposé une plainte relative aux droits de la personne contre son employeur sur la question de l'obligation de prendre des mesures d'adaptation dans une situation d'invalidité médicale. Dans le cadre de l'enquête que le Commissariat a effectuée sur les circonstances ayant mené au dépôt d'une plainte relative aux droits de la personne, une autre question est entrée en jeu, à savoir si l'employée avait occupé un autre emploi pendant son congé d'invalidité.

Conformément aux principes de base sur l'équité des procédures applicables aux enquêtes, les enquêteurs sont tenus d'expliquer la nature et la portée de leur enquête afin d'obtenir de l'information juste et appropriée.

Afin de vérifier les faits, la SCP a communiqué avec l'autre organisme pour en savoir davantage sur les fonctions de la plaignante. La SCP a informé l'organisme qu'elle faisait enquête par suite d'une plainte relative aux droits de la personne déposée contre elle sur la question du congé d'invalidité; elle lui a indiqué la nature de l'information qu'elle souhaitait obtenir. Avant de communiquer à la SCP de l'information sur la plaignante, l'organisme a demandé à celle-ci son consentement et a fait allusion au congé d'invalidité qu'elle aurait obtenu. Nous avons toutefois conclu que l'organisme avait déduit cette situation, puisque rien n'indiquait que la SCP ait mentionné que la plaignante avait pris un congé d'invalidité.

Puisque les renseignements que la SCP a fournis à l'organisme au sujet de la plaignante étaient nécessaires et directement liés à la tenue de l'enquête sur la

renseignements sur l'entreprise à laquelle il est associé. Il s'opposait également à ce que la prestation des renseignements personnels soit obligatoire en dépit d'un avis du MAECI concernant la protection de la vie privée selon lequel la prestation des renseignements personnels était facultative.

Le Commissariat a appris que le MAECI demandait aux abonnés canadiens de son bulletin électronique de fournir leur adresse électronique, le nom de leur ville et de leur province de résidence, leur code postal, leur numéro de téléphone et des renseignements sur l'entreprise à laquelle ils sont associés. Les abonnés étrangers devaient uniquement fournir leur adresse électronique et le nom de leur pays d'origine. Nous avons pu confirmer que la demande d'abonnement était refusée en l'absence de ces renseignements.

Le MAECI a expliqué que les numéros de téléphone étaient nécessaires pour communiquer avec les abandonnés dans l'éventualité de problèmes techniques avec les adresses électroniques. Les codes postaux et les renseignements sur l'entreprise servaient à cibler une région ou un type d'entreprise pour la transmission de communiqués. Le Commissariat a conclu qu'en vertu de la Loi, le MAECI était autorisé à recueillir des renseignements sur les abonnés afin de faciliter l'accès aux communiqués et leur diffusion. La plainte a donc été jugée non fondée. Nous étions toutefois satisfaits de savoir que le MAECI reconnaissait que l'emploi du mot « facultatif » dans les avis portait à confusion; il s'agissait en réalité du processus d'inscription à l'abonnement qui était facultatif. Le MAECI a depuis modifié ses avis en conséquence.

Obligation injustifiée de fournir le numéro d'assurance sociale

Une gardienne d'enfant a porté plainte après que le père d'un enfant dont elle prenait soin a exigé qu'elle fournisse son numéro d'assurance sociale (NAS). Le père avait besoin de ce numéro afin d'obtenir un remboursement dans le cadre du programme d'aide aux familles pour les services de garde du ministère de la Défense nationale (MDN).

En vertu de ce programme, certains membres des Forces canadiennes peuvent obtenir le remboursement des frais de garde de leurs enfants lorsqu'ils sont en service loin de la maison. Pour profiter de ce programme, les membres doivent présenter des reçus et remplir un formulaire du MDN dans lequel on demande des renseignements sur la personne qui garde l'enfant, dont son nom, numéro d'assurance sociale ou numéro d'entreprise.

Les durées de traitement ci-dessus constituent une source de préoccupation : il s'écoule en moyenne 10,5 mois entre la date de réception d'une plainte et la date à laquelle une conclusion est formulée. La ventilation par conclusion indique que les plaintes donnant lieu à une enquête complète – c'est-à-dire celles appartenant aux catégories *fondée et résolue, réglée, non fondée et réglée en cours d'enquête* – exigent en moyenne plus d'une année de travail. Le temps de traitement des plaintes dites *régles* témoigne de la pratique de longue date du Commissariat qui est de ne pas considérer un cas réglé tant que l'enquête n'est pas officiellement terminée. Toutefois, il nous fait plaisir d'annoncer un changement à cette pratique : une plainte peut désormais être *réglée* à n'importe quel moment pendant l'enquête, ce qui devrait réduire le temps de traitement des plaintes *régles*.

Suivi après l'enquête

Le traitement d'une plainte ne se termine pas nécessairement à la fin de l'enquête. Toutes les plaintes pour collecte, utilisation, communication ou conservation inappropriée de renseignements personnels qui sont jugées fondées sont envoyées à la Direction de la vérification et de la revue pour être examinées. La Direction peut ainsi déceler des tendances et établir des modèles de comportement liés à des situations d'atteinte à la protection de la vie privée, et utiliser les résultats des examens pour la planification et l'élaboration des vérifications de l'année à venir.

Cas choisis – Loi sur la protection des renseignements personnels

Les résumés de cas ci-dessous constituent un échantillon des plaintes déposées auprès du Commissariat et exemplifient l'approche adoptée pour traiter différentes questions relatives à la protection des renseignements personnels dans le secteur public. Ces cas démontrent à quel point il est important pour les institutions et les organismes gouvernementaux de faire preuve de vigilance dans le traitement des renseignements personnels; un manque de vigilance peut entraîner des conséquences néfastes, comme ces cas en témoignent.

Abonnés obligés de fournir des renseignements pour renouveler un abonnement à un bulletin électronique de nouvelles

Un abonné d'un service de bulletin électronique de nouvelles a porté plainte pour avoir dû fournir plus de renseignements que nécessaire afin de renouveler son abonnement. L'abonnement était offert par le ministère des Affaires étrangères et du Commerce international (MAECI). Plus particulièrement, le plaignant refusait de fournir son code postal, son numéro de téléphone et des

Durée de traitement des enquêtes faisant suite à des plaintes – Loi sur la protection des renseignements personnels

Les tableaux ci-dessous indiquent la durée moyenne (en mois) d'une enquête faisant suite à une plainte, à compter de la date de réception de la plainte jusqu'à la date à laquelle une conclusion est formulée. Le premier tableau donne une ventilation par conclusion; le deuxième, par type de plainte.

Par conclusion

Pour la période du 1^{er} avril 2005 au 31 mars 2006.

Conclusion		Durée de traitement moyen (en mois)
Réglée rapidement		3,61
Fondée		7,18
Non fondée		13,22
Abandonnée		8,96
Réglée en cours d'enquête		16,46
Fondée et résolue		23,09
Résolue		14,27
Moyenne générale		10,49

Par type de plainte

Pour la période du 1^{er} avril 2005 au 31 mars 2006.

Type de plainte		Durée de traitement moyen (en mois)
Correction/annotation - délais		9,20 *
Avis de prorogation		8,45
Délais		6,49
Accès		15,14
Langue		25,00 **
Utilisation et communication		14,25
Collecte		14,64
Conservation et retrait		23,86
Correction/annotation		9,73
Moyenne générale		10,5

* Le délai de traitement pour ce genre de plainte se fonde sur cinq cas.
 ** Le délai de traitement pour ce genre de plainte se fonde sur un seul cas.

Plaintes fermées - délais
Du 1^{er} avril 2005 au 31 mars 2006

	Abandonnée	Réglée rapidement	Non fondée	Réglée	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
--	------------	-------------------	------------	--------	---------------------------	--------	-------------------	-------

Correction/annotation - délais	0	0	0	0	0	5	0	5
Avis de prorogation	2	1	37	0	0	4	0	44
Délais	47	5	22	11	8	395	0	488
Total	49	6	59	11	8	404	0	537

Il est important de souligner que parmi les 537 plaintes déposées, 75 % étaient fondées. Étant donné leur nature, la majorité des plaintes liées aux délais sont fondées. Les institutions disposent de 30 jours, à compter de la date de réception des demandes, pour fournir aux personnes qui en font la demande l'accès à leurs renseignements personnels. En général, personne ne dépose ce genre de plainte à moins qu'il y ait eu un retard dans le traitement de la demande. Les exceptions faisant en sorte qu'une telle plainte serait jugée non fondée concernent soit les situations où une prorogation légitime accorde un délai additionnel de 30 jours pour répondre à une demande, soit les situations où les plaignants n'ont pas prévu le temps d'expédition par la poste. En effet, le délai de 30 jours commence à la date à laquelle l'institution reçoit la demande de renseignements.

Le CPVP demeure toutefois préoccupé par le nombre de plaintes liées aux délais déposées contre certaines institutions, bien que plusieurs d'entre elles aient pris des mesures afin de combler le manque de ressources. Il est notoire que le processus de dotation dans la fonction publique est considérablement long, tout comme la formation des nouveaux employés. Il subsiste donc un décalage entre le moment où l'on détermine les besoins en ressources et celui où l'on réussit à augmenter la productivité et à réduire les arriérés. Le CPVP continuera, au cours de la présente année, à surveiller le respect des délais prévus par la Loi sur la protection des renseignements personnels.

L'annexe 1 donne une ventilation détaillée, par ministère, des plaintes liées aux délais.

Plaintes fermées - accès et protection des renseignements personnels

Du 1^{er} avril 2005 au 31 mars 2006

Abandonnée	Réglée rapidement	Non fondée	Réglée	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
54	12	143	12	63	1	23	308
2	2	19	0	9	1	0	33
24	1	3	0	5	0	0	33
0	0	0	1	0	0	0	1
0	0	2	0	4	1	0	7
12	2	51	2	29	25	0	121
92	17	218	15	110	28	23	503
Total							
Accès							
Collecte							
Correction/annotation							
Langue							
Conservation et retrait							
Utilisation et communication							

Le tableau montre clairement qu'il y a beaucoup plus de plaintes non fondées que de plaintes fondées : 218 et 51 respectivement. Ce nombre inclut les plaintes fondées et résolues. De plus, un grand nombre de plaintes sont réglées d'une façon ou d'une autre (abandonnées, réglées rapidement, réglées ou réglées en cours d'enquête) : 234 plaintes sur 503, soit 47 %. En examinant les résultats, nous pouvons conclure que seulement 10 % des plaintes adressées au Commissariat sont fondées. Selon nous, ces chiffres démontrent clairement que les institutions fédérales observent généralement la Loi.

L'annexe 1 donne une ventilation détaillée, par ministère, des plaintes relatives à l'accès ou à la protection des renseignements personnels qui ont été fermées.

Réglée : après une enquête approfondie, le Commissariat a participé à la négociation d'une solution satisfaisant les deux parties. Cette conclusion est réservée aux plaintes qu'on pourrait difficilement qualifier de fondées du fait que la situation relève essentiellement d'une mauvaise communication ou d'un malentendu.

Réglée en cours d'enquête : le Commissariat a participé à la négociation d'une solution satisfaisant toutes les parties dans le cadre de l'enquête. Aucune conclusion n'est rendue.

Abandonnée : l'enquête a pris fin avant que toutes les allégations soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons. Par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire, ou il est impossible de le trouver afin qu'il fournisse des renseignements supplémentaires essentiels pour arriver à une conclusion.

Conclusions selon le type de plainte

Les tableaux ci-dessous donnent les résultats de nos enquêtes selon les différents types de plaintes que nous recevons. Le premier tableau donne tous les types de plaintes; le deuxième représente les plaintes relatives à l'accès et à la protection des renseignements personnels; le troisième tableau présente les plaintes strictement liées aux délais. Nous présentons nos statistiques ainsi réparties pour la première fois afin d'illustrer le nombre important de plaintes liées aux délais.

Plaintes fermées - tous les types de plaintes

Du 1^{er} avril 2005 au 31 mars 2006

Abandonnée	Réglée rapidement	Non fondée	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
54	12	143	12	63	1	308
2	2	19	0	9	1	33
24	1	3	0	5	0	33
Correction/annotation						
0	0	0	0	5	0	5
Correction/annotation - délais						
2	1	37	0	4	0	44
Avis de prorogation						
0	0	0	1	0	0	1
Conservation et retrait						
0	0	2	0	4	1	7
Délais						
47	5	22	11	8	395	488
Utilisation et communication						
12	2	51	2	29	25	121
141	23	277	26	118	432	1 040
Total						

Plaintes traitées entre le 1^{er} avril 2005 et le 31 mars 2006

Au cours du dernier exercice, nous avons traité 1 040 plaintes, soit à peu près le nombre de plaintes que nous avons reçues pendant cette période.

Bien que le Commissariat ait traité autant de plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels* qu'il en a reçu, il procède, en fin d'exercice, au suivi d'un nombre considérable de cas – soit 1 263. La conduite d'un examen approfondi des processus opérationnels de la Direction en début d'année a permis d'évaluer les ressources nécessaires et de trouver des moyens de traiter notre charge de travail accumulée. L'examen a également permis de déterminer un besoin en ressources supplémentaires. Aussi, d'intenses procédures de dotation ont été amorcées en vue du recrutement, d'embaucher et de former de nouveaux enquêteurs. Nous sommes déterminés à traiter l'arrière de cas d'ici deux ans.

Définitions des conclusions et d'autres dispositions en vertu de la *Loi sur la protection des renseignements personnels*

Le Commissariat a élaboré une série de définitions de conclusions qui expliquent les résultats des enquêtes qu'il effectue en vertu de la *Loi sur la protection des renseignements personnels*.

Réglée rapidement : s'applique aux cas où l'affaire est réglée avant même qu'une enquête officielle ne soit entamée. Par exemple, si une personne dépose une plainte dont le sujet a déjà fait l'objet d'une enquête par le Commissariat et a été considéré conforme à la *Loi sur la protection des renseignements personnels*, nous expliquons la situation à cette personne. Il nous arrive également de recevoir des plaintes pour lesquelles une enquête officielle aurait pu avoir des conséquences défavorables pour la personne. En pareil cas, nous expliquons en détail la situation au plaignant. Si ce dernier décide de ne pas poursuivre l'affaire, celle-ci est jugée « réglée rapidement ».

Non fondée : l'enquête n'a pas permis de déceler des éléments de preuve qui suffisent à conclure que l'institution fédérale n'a pas respecté des droits d'un plaignant selon la *Loi sur la protection des renseignements personnels*.

Fondée : l'institution fédérale n'a pas respecté les droits d'une personne aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée et résolue : les allégations sont corroborées par l'enquête et l'institution fédérale accepte de prendre des mesures correctives afin de remédier à la situation.

Plaintes reçues selon leur origine

Du 1^{er} avril 2005 au 31 mars 2006

Le tableau ci-dessous montre la province ou le territoire d'origine des plaintes reçues au cours de la période visée par le rapport. À noter que certaines plaintes reçues ont été déposées par des personnes vivant à l'extérieur du Canada. La Loi sur la protection des renseignements personnels couvre également les renseignements personnels que détient le gouvernement du Canada sur des Canadiennes et des Canadiens vivant à l'étranger.

Province/Territoire	Total	Pourcentage
---------------------	-------	-------------

Québec	249	24,00
Ontario	225	22,00
Colombie-Britannique	182	18,00
RCN	159	15,00
Alberta	68	7,00
Manitoba	53	5,00
Saskatchewan	35	3,00
International	17	2,00
Nouveau-Brunswick	15	1,50
Nouvelle-Écosse	16	16,00
Terre-Neuve	5	0,50
Ile-du-Prince-Édouard	2	0,20
Territoire du Yukon	2	0,20
Total	1 028	100,00

Près de 80 % des plaintes proviennent des provinces du Québec, de l'Ontario et de la Colombie-Britannique, ainsi que de la région de la capitale nationale. Cette tendance correspond à ce que nous avons constaté au cours des cinq dernières années, c'est-à-dire que le Québec, l'Ontario et la Colombie-Britannique sont, à une exception près, les provinces d'où proviennent la grande majorité des plaintes reçues. L'exception ci-mentionnée est survenue au cours de l'exercice 2003-2004 : l'Alberta, et non l'Ontario, occupait la troisième place.

Plaintes reçues par institution gouvernementale

Le tableau ci-dessous indique le nombre réel de plaintes déposées contre les institutions et organismes gouvernementaux au cours de l'exercice se terminant le 31 mars 2006.

Total	1 028
Administration canadienne de la sûreté du transport aérien	2
Administration de pilotage du Pacifique	1
Affaires étrangères et Commerce international Canada	33
Affaires indiennes et du Nord Canada	3
Agence canadienne d'inspection des aliments	1
Agence de développement économique du Canada pour les régions du Québec	13
Agence des services frontaliers du Canada	34
Agence du revenu du Canada	92
Agriculture et Agroalimentaire Canada	32
Anciens Combattants Canada	6
Bibliothèque et Archives Canada	7
Bureau du Commissaire des tribunaux de révision	1
Bureau du Conseil privé	1
Centre des armes à feu Canada	1
Citoyenneté et Immigration Canada	60
Commission canadienne des droits de la personne	4
Commission d'appel des pensions	2
Commission de la fonction publique du Canada	7
Commission de l'immigration et du statut de réfugié du Canada	121
Commission des plaintes du public contre la GRC	1
Commission nationale des libérations conditionnelles	4
Conseil national de recherches Canada	2
Défense nationale	41
Développement social Canada	13
Elections Canada	1
Exportation et Développement Canada	8
Gendarmerie royale du Canada	165
Industrie Canada	5
Justice Canada	29
L'Enquêteur correctionnel Canada	1
Musée des beaux-arts du Canada	1
Patrimoine canadien	1
Pêches et Océans Canada	1
Résolution des questions des pensionnats indiens Canada	1
Ressources humaines et Développement des compétences Canada	35
Santé Canada	18
Sécurité publique et Protection civile Canada	1
Service canadien du renseignement de sécurité	35
Service correctionnel Canada	190
Société canadienne des postes	42
Statistique Canada	3
Transports Canada	3
Travaux publics et Services gouvernementaux Canada	6
Total	1 028

Les dix institutions ayant reçu le plus de plaintes, par type de plainte.
Le tableau ci-dessous présente les institutions gouvernementales ayant reçu le plus de plaintes au cours de l'exercice se terminant le 31 mars 2006.

Organisme	Total	Accès	Délais	Protection des renseignements personnels
-----------	-------	-------	--------	--

Service correctionnel Canada	190	108	43	39
Gendarmerie royale du Canada	165	35	121	9
Commission de l'immigration et du statut de réfugié du Canada*	121	32	85	4
Agence du revenu du Canada	92	38	37	17
Citoyenneté et Immigration Canada	60	32	27	1
Société canadienne des postes	42	15	17	10
Défense nationale	41	13	21	7
Ressources humaines et Développement des compétences	35	10	5	20
Service canadien du renseignement de sécurité	35	30	5	0
Agence des services frontaliers du Canada	34	12	19	3
Autres	213	111	62	40
Total	1 028	436	442	150

* Un grand nombre des plaintes visant la Commission de l'immigration et du statut de réfugié du Canada ont été déposées par une seule et même personne.

Le nombre de plaintes visant les institutions ne signifie pas que celles-ci ne respectent pas la *Loi sur la protection des renseignements personnels*. En raison de leur mandat, certaines de ces institutions détiennent une quantité considérable de renseignements personnels sur des citoyens; elles sont donc plus susceptibles de recevoir de nombreuses demandes d'accès à ces renseignements personnels. Compte tenu du volume de renseignements qu'elles détiennent, on peut s'attendre à ce que ces institutions fassent l'objet d'un plus grand nombre de plaintes concernant la collecte, l'utilisation, la communication, la conservation et la destruction de renseignements personnels, ainsi que de plaintes relatives à l'accès aux renseignements personnels.

Délais :

- **Délais** - L'institution n'a pas répondu dans les délais prescrits.
- **Avis de prorogation** - L'institution n'a pas donné une justification appropriée pour la prorogation; elle a fait la demande de prorogation après le délai initial de 30 jours, ou elle a fixé l'échéance à plus de 60 jours de la date de réception de la demande.
- **Correction/annotation - délais** - L'institution n'a pas corrigé les renseignements personnels ou n'a pas annoté le dossier dans les 30 jours suivant la réception de la demande de correction.

Plaintes reçues entre le 1^{er} avril 2005 et le 31 mars 2006

En 2005-2006, le Commissariat a reçu 1 028 plaintes, soit 549 plaintes de moins qu'au cours de l'exercice précédent. À cette diminution de 35 % par rapport à l'exercice précédent correspond un nombre moins élevé de plaintes relatives à l'accès aux renseignements personnels, à leur utilisation et à leur communication ainsi qu'aux délais pour l'obtention de renseignements. Contrairement à l'exercice précédent, le Commissariat n'a pas reçu de groupes de plaintes, d'où, possiblement, la diminution du nombre de plaintes reçues.

Type de plainte	Nombre	Pourcentage
Accès	391	38,00
Collecte	25	2,40
Correction/annotation	44	4,30
Correction/annotation - délais	9	0,90
Avis de prorogation	22	2,10
Langue	1	0,10
Conservation et retrait	10	1,00
Délais	411	40,00
Utilisation et communication	115	11,20
Total	1 028	100,00

À l'instar des années précédentes, le type de plainte le plus courant est le non-respect des institutions du délai de trente jours prévu par la Loi pour répondre aux demandes d'accès à des renseignements personnels. Les plaintes pour non-respect du délai, ainsi que les plaintes pour refus d'accès à des renseignements personnels et pour utilisation et communication inappropriées de renseignements personnels, représentent 89 % du nombre total de plaintes reçues. Les chiffres de l'exercice 2004-2005 montrent une répartition similaire, ces types de plainte représentant alors 85 % du total.

- ou des renseignements ou encore parce que l'organisation a invoqué des exceptions afin de ne pas communiquer les renseignements.
- **Correction/annotation** - L'institution n'a pas apporté les corrections aux renseignements personnels ou ne les a pas annotés parce qu'elle n'approuve pas les corrections demandées.
- **Langue** - Les renseignements personnels n'ont pas été fournis dans la langue officielle demandée.
- **Frais** - Des frais ont été exigés pour répondre à la demande de renseignements effectuée en vertu de la *Loi sur la protection des renseignements personnels*; aucun frais n'est présentement prévu pour l'obtention de renseignements personnels.
- **Répertoire** - InfoSource¹ ne décrit pas de façon adéquate le fonds de renseignements personnels que détient une institution.

Protection des renseignements personnels :

- **Collecte** - Une institution a recueilli des renseignements personnels qui ne sont pas nécessaires à l'exploitation d'un de ses programmes ou à l'une de ses activités; les renseignements personnels n'ont pas été recueillis directement auprès de la personne concernée; ou la personne n'a pas été informée des fins pour lesquelles les renseignements personnels ont été recueillis.

- **Conservation et retrait** - Des renseignements personnels ne sont pas conservés selon les calendriers de conservation et de destruction (approuvés par les Archives nationales et publiés dans InfoSource) : ils sont détruits trop rapidement ou conservés trop longtemps.
- De plus, les renseignements personnels utilisés à des fins administratives doivent être conservés pendant au moins deux ans après la dernière application d'une mesure administrative, à moins que la personne n'ait consenti à leur retrait.

- **Utilisation et communication** - Des renseignements personnels sont utilisés ou communiqués sans le consentement de la personne qu'ils concernent et ne satisfont pas à l'un des critères de communication permise sans consentement, tels qu'énoncés au paragraphe 8(2) de la Loi.

¹ InfoSource est un répertoire du gouvernement fédéral qui décrit chaque institution et les banques de données (groupes de fichiers sur un même sujet) que celle-ci possède.

Depuis 1983, le Commissariat à la protection de la vie privée du Canada enquête sur des plaintes relatives à des renseignements personnels détenus par les ministères et organismes fédéraux. La *Loi sur la protection des renseignements personnels* (la Loi) régit la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels dans le cadre de l'administration des programmes gouvernementaux, et accorde aux citoyens le droit d'accéder aux renseignements personnels que le gouvernement détient à leur sujet. La commissaire à la protection de la vie privée du Canada traite habituellement les plaintes déposées par des citoyens, mais elle peut de sa propre initiative, également, déposer elle-même une plainte ou enquêter lorsqu'une situation lui donne des motifs raisonnables de croire qu'il y a eu infraction à la *Loi sur la protection des renseignements personnels*.

La commissaire à la protection de la vie privée est un ombudsman qui règle les plaintes par, dans la mesure du possible, la médiation, la négociation et les discussions persuasives. Toutefois, la Loi lui confère de vastes pouvoirs d'enquête pour mener à bien son mandat. La commissaire peut assigner et contraindre des témoins à comparaître; elle peut pénétrer dans des locaux pour obtenir des documents ou mener des entrevues. Elle peut également émettre des recommandations – ce qu'elle fait régulièrement – visant à modifier les pratiques de traitement des renseignements personnels des institutions gouvernementales.

Définition des types de plaintes

Les plaintes adressées au Commissariat sont réparties en trois grandes catégories :

- **Accès** - Une personne n'a pas obtenu tous les renseignements personnels qu'une institution détient à son sujet parce qu'il manque des documents

vigilance éternelle. Jusqu'où la soif d'identification et de surveillance des transactions nous mènera-t-elle? Nous est-il possible de gérer cette diversité d'activités et d'en arriver à établir une approche relative à l'identité et à l'authentification que nous oserions qualifier de complète?

Nous allons certainement essayer. Beaucoup d'efforts ont été déployés en ce sens dans d'autres juridictions. Nous nous réjouissons de savoir que le Secrétariat du Conseil du Trésor se penche sur certains de ces enjeux au Canada et nous espérons pouvoir faire notre part en présentant notre point de vue à l'égard de la protection de la vie privée. Les enjeux relatifs à l'identité demeurent néanmoins une question complexe.

relatifs à la vie privée concernant ce projet, nous procédons actuellement à l'examen de ce dernier.

Dans ses activités quotidiennes habituelles, le gouvernement fédéral travaille à l'amélioration de la prestation de services électroniques. Service Canada s'efforce de mettre en œuvre la prestation de services intégrée afin d'offrir aux Canadiennes et aux Canadiens quelque chose qui ressemble au « guichet unique » que l'on trouve actuellement dans les supermarchés. L'architecture qui sous-tend ces groupes de services continuera de nous mettre à l'épreuve dans nos efforts pour simplifier le processus sans favoriser la création d'une architecture panoplique grâce à laquelle l'autorité centrale, le gouvernement, peut tout voir.

Les chefs de file des technologies de l'information, comme Microsoft et IBM, présentent entre autres, de nouveaux cadres de gestion de l'identité permettant de composer avec les problèmes liés à la fraude, aux pourriels et à la convivialité, entre autres. Les sociétés de télécommunications, réagissant à nos propres préoccupations en ce qui concerne la communication de renseignements personnels uniquement à la personne concernée, mettent au point de nouveaux modes d'authentification plus rigoureux. Le gouvernement demande aux banques de fournir davantage de données au sujet des personnes et de leurs transactions. En prévision de l'examen de la Loi en 2006, nous avons examiné les dispositions législatives régissant la déclaration des crimes financiers, et nous demeurons préoccupés par les pouvoirs de surveillance des transactions financières que prévoit cette loi. Combien de Canadiennes et de Canadiens savent vraiment où se retrouvent les données financières les concernant et ce qu'il advient de l'information communiquée par les banques, les comptables, les avocats et d'autres intervenants du secteur privé au sujet de leurs clients? Même si les données étaient gérées parfaitement et que nous avions le temps d'en arriver à la conclusion que ces données font bel et bien l'objet d'une gestion efficace au moyen de vérifications des intervenants désignés, il n'en demeure pas moins que, dans notre démocratie, très peu de personnes saisissent l'ampleur de la croissance des activités de surveillance et de collecte de données, ce qui demeure en soi source d'inquiétudes.

À l'occasion, lorsque nous rencontrons nos collègues du gouvernement afin de discuter de nouvelles initiatives, nous posons des questions qui peuvent sembler quelque peu choquantes. Le Canada n'est d'aucune façon un État oppressif, et les représentants du gouvernement fédéral nous impressionnent énormément par leur désir de maintenir la protection de la vie privée, de comprendre les répercussions d'infrastructures technologiques complexes, et par leur respect à l'égard des droits de la personne et des libertés civiles. Mais le prix de la liberté est, effectivement, la

depuis l'analyse de l'utilisation du numéro d'assurance sociale jusqu'au mémoire du Commissariat sur la carte d'identité biométrique. Cette année, nous avons décidé de faire de la gestion de l'identité le prochain élément central du programme de la Direction de la recherche et des politiques. Voici quelques exemples d'expériences réalisées en 2005-2006 qui nous ont menés à cette conclusion.

Nous avons été submergés par les enjeux liés à la sécurité frontalière : nous avons effectué une vérification de l'Agence des services frontaliers du Canada, présentée plus loin dans le présent rapport; nous avons fait part de nos observations sur les multiples théories relatives à la carte frontalière canado-américaine proposée; nous avons posé des questions à Transports Canada concernant les listes de zones d'interdiction aérienne. Même s'il est tout à fait légitime pour un état souverain de vouloir confirmer l'identité des personnes qui entrent sur son territoire, nous craignons qu'une telle carte, une fois établie, soit exigée dans une foule de nouvelles situations. Nous avons remarqué que la crainte à l'égard d'activités terroristes et criminelles éventuelles nous pousse à vouloir faire la lumière sur tout et à tout vouloir identifier, comme le ferait un enfant qui craint l'obscurité. Il n'a pourtant pas été démontré clairement que l'identification de chaque individu nous permettrait de distinguer les bons des mauvais, bien que dans certains cas, l'identification pourrait effectivement aider à prévenir la fraude. Néanmoins, nous consacrons une part considérable de notre temps à disséquer les raisons d'être de ces nouvelles cartes, des nouveaux systèmes de gestion de l'identité, des nouveaux registres de personnes, et à réagir à la perte progressive de l'anonymat dans les transactions de la vie quotidienne.

On pourrait évidemment remarquer que, en ce qui concerne les listes de zones d'interdiction aérienne, par exemple, si une personne est trop dangereuse pour se trouver à bord d'un avion, elle risque d'être également trop dangereuse pour monter à bord d'un métro ou d'un train. Or nous mènera ce genre de réflexion? Lorsqu'on se penche sur l'utilisation, dans d'autres juridictions, de puces d'IRF insérées aux plaques d'immatriculation de véhicules motorisés permettant de suivre les allées et venues des véhicules sur les routes et les autoroutes, n'est-il pas normal de se demander si ces dispositifs finiront par être incorporés aux personnes? Ces questions méritent d'être posées; sans doute est-il de notre devoir de le faire.

À l'égard des questions que nous avons fait parvenir à Transports Canada au sujet de la liste de zones d'interdiction aérienne, la commissaire a affirmé publiquement, en août 2005, que cette liste pourrait constituer une « grave immixtion entravant les droits des voyageurs au Canada, le droit à protection de la vie privée et le droit à la liberté de mouvement ». En mai 2006, nous avons reçu une évaluation des facteurs

La gestion de l'identité compte parmi les principaux thèmes étudiés dans le cadre des analyses de la recherche et des politiques menées cette année. Au cours des 23 dernières années, le Commissariat s'est penché sur ce sujet sous divers angles,

Gestion de l'identité et lutte contre le crime et la terreur

allons-nous élaborer d'autres directives à cet égard.

Nous avons constaté un intérêt croissant pour la vidéosurveillance au Canada; aussi, Web, rendent certainement possibles la création de puissants réseaux de surveillance. à la facilité avec laquelle les caméras à distance peuvent maintenant être liées au reconnaissance faciale et de reconnaissance des habitudes migratoires, le tout associé réduction des coûts de stockage de données, la conception de logiciels efficaces de pipelines aux sites nucléaires. L'augmentation de la puissance de ces caméras, la d'installations pour lesquels la protection de l'infrastructure est essentielle, des publics, mais aussi dans les magasins, les lieux de travail et presque tous les types qui permettent d'effectuer facilement ce genre de surveillance dans les lieux continuons à examiner l'utilisation accrue des caméras et les progrès technologiques publics. Nous avons affiché ces lignes directrices dans notre site Web et nous (GRC) à l'élaboration de lignes directrices sur la surveillance vidéo dans les lieux Le Commissariat a travaillé en collaboration avec la Gendarmerie royale du Canada

Lignes directrices en matière de vidéosurveillance

l'année.

et nous préparons actuellement d'autres directives qui seront publiées au cours de passage à la frontière. Nous avons versé une fiche d'information à notre site Web secteur public, il a été suggéré d'intégrer des AIRF aux passeports et aux cartes de d'un usage très répandu dans les produits de consommation au Canada. Quant au modes d'application de nos lois à cet effet. Ces dispositifs pourraient faire l'objet protection de la vie privée des appareils d'identification par radiofréquence et des Nous procédons depuis un certain temps à l'analyse de l'incidence potentielle sur la

Appareils d'identification par radiofréquence (AIRF)

d'échanger des connaissances et de créer des liens efficaces. façon très utile et relativement peu coûteuse d'élaborer des approches harmonisées, à travailler avec nos collègues à l'élaboration d'un programme d'échanges, une rencontrer et de profiter de l'expertise des différents participants. Nous continuerons gouvernement, du secteur privé, de la société civile et du milieu universitaire de se excellente occasion pour les Canadiennes et les Canadiens du / en provenance du

transfrontalière de leurs renseignements personnels et quant aux risques éventuels à la protection de la vie privée que présentent des lois étrangères, telle la *USA PATRIOT Act* ou es cas d'absence de lois de protection des données personnelles. Les données personnelles circulent de plus en plus sur le globe terrestre puisqu'elles constituent une partie importante de l'économie mondiale. Les règles internationales de protection des données, comme celles de l'OCDE et de l'Union européenne, ont été mises sur pied pour faciliter le transfert des données outre-frontières dans les conditions jugées appropriées. Les dernières lignes directrices du Conseil du Trésor visaient à rencontrer les mêmes objectifs et nous espérons qu'elles feront partie intégrante dans l'actualisation de la *Loi sur la protection des renseignements personnels*.

Relations internationales

Au cours de la dernière année, nous avons reçu à plusieurs reprises des collègues d'autres pays afin de nous entretenir sur nos expériences respectives dans le domaine de la protection des données et de contribuer à l'élaboration de lois sur la protection des données. Avec la circulation internationale des données, il est de plus en plus important que, nonobstant différentes approches juridiques, nous atteignons des résultats harmonisés dans nos attentes sur le plan des activités de protection. Il sera important, pour nos échanges de données sur les citoyens, de pouvoir compter sur la surveillance effectuée par des autorités similaires à l'extérieur de notre juridiction afin de garantir la protection de la vie privée des Canadiennes et des Canadiens.

En octobre et novembre, nous avons reçu / étions l'hôte d'un analyste de politiques de la Commission nationale de l'information et des libertés (CNIL) l'autorité indépendante de la France. Ce fut un honneur de recevoir le président de la CNIL, Monsieur Alex Türk; nous avons pu comparer nos différentes approches concernant l'application de la loi. En décembre, nous avons accueilli deux agents principaux de l'institut fédéral mexicain pour l'accès aux renseignements publics, qui voulaient connaître le fonctionnement de base de notre système. En effet, le Mexique envisage d'adopter une loi en matière de protection des données; il a soumis un projet de loi au Congrès mexicain. Après la visite de ces deux représentants, nous nous sommes préparés à la visite d'une délégation plus nombreuse venue passer trois jours au Canada en mai 2006.

Nous attendons avec impatience la Conférence internationale des commissaires à la protection des données et de la vie privée dont nous serons les hôtes en septembre 2007. À cette occasion, de nombreux spécialistes de la protection de la vie privée et des données se rencontreront à Montréal. Cette conférence sera une

accepté de siéger à un comité de l'Organisation de coopération et de développement économiques (OCDE) qui enquête sur la nécessité d'une meilleure collaboration entre autorités indépendantes pour le traitement des infractions transfrontalières aux lois sur la protection des données.

Le Commissariat a traité des plaintes relatives au marketing international de renseignements personnels; il avertit que les enjeux juridiques deviendront une source de préoccupation croissante dans le domaine de la protection des données, à l'instar du cybercrime. Le ministre de la Justice du gouvernement précédent avait fait part de son appui à la ratification du Traité sur le cybercrime du Conseil de l'Europe, dont l'objet est de favoriser la collaboration entre les signataires dans la lutte contre le crime international. Il faut que cette entente comporte aussi des modalités en matière de protection de la vie privée, ou alors il nous faudra disposer d'outils administratifs tels les traités d'entraide juridique et les protocoles d'entente avec d'autres pays.

Nous avons donné suite aux débats de 2004 sur la circulation transfrontalière des données au début de 2005, par une lettre au président du Conseil du Trésor exhortant le gouvernement fédéral à examiner les répercussions du recours à l'impartition pour traiter les renseignements personnels, ainsi qu'à assortir les contrats de clauses relatives à la protection des renseignements personnels dont le traitement est confié à des tiers. Dans les mois qui suivirent, le Secrétaire du Conseil du Trésor nous a consulté à propos de sa stratégie fédérale visant à donner suite aux préoccupations en matière de protection de la vie privée relatives à la *USA PATRIOT Act*, et avançait la possibilité que des lois étrangères minent la protection des renseignements personnels de la population canadienne. L'évaluation des contrats d'impartition par les 160 institutions fédérales a révélé que plus de 80% d'entre elles ont classé leurs ententes d'impartition dans les catégories « risques inexistant » et « risques faible ». Cette évaluation a également aidé les ministres et organismes à identifier les mesures visant à atténuer les risques en matière de protection des renseignements personnels. L'un des documents clés du Secrétaire du Conseil du Trésor présentait un ensemble de lignes directrices destinées aux institutions gouvernementales. Ces lignes directrices établissent des règles à l'égard des activités d'impartition dans le cadre desquelles des renseignements personnels concernant des Canadiens sont traités ou obtenus par des organismes du secteur privé en vertu d'un contrat conclu avec une institution gouvernementale.

À notre avis, la stratégie fédérale progresse vers l'objectif de répondre adéquatement aux préoccupations de la population canadienne quant à la circulation

pas de lui-même mais bien du responsable de l'institution. Nous encourageons les organismes gouvernementaux à rappeler à leurs porte-parole de donner cette réponse dans les cas de demandes de renseignements personnels.

Circulation transfrontalière des données

L'année dernière, nous avons abordé les préoccupations formulées par des Canadiennes et des Canadiens relativement à l'incidence de la *USA PATRIOT Act* sur les renseignements que détiennent des entreprises situées aux États-Unis. La *USA PATRIOT Act* cristallise la préoccupation croissante des Canadiennes et des Canadiens à l'égard de la sécurité de leurs renseignements personnels lorsque ces renseignements quittent le pays. La *USA PATRIOT Act*, adoptée rapidement par le Congrès américain, peu après les événements du 11 septembre 2001, comporte d'un certain nombre de dispositions qui devaient cesser d'être en vigueur après cinq ans, à moins que le gouvernement américain ne convainque le Congrès de les rendre permanentes; ce qu'il a fait en mars 2006. Les dispositions controversées sont maintenant permanentes. Le Commissariat a certes fait part de ses préoccupations à l'égard de notre propre *Loi antiterroriste* dans les rapports annuels antérieurs; il a aussi signalé l'inquiétude croissante à l'égard de l'incidence des lois étrangères sur les données personnelles qui quittent le territoire canadien.

Cette question a certainement affecté les Canadiennes et les Canadiens, lesquels nous ont adressé des questions et des plaintes au sujet de la menace à l'égard de leur droit à la vie privée que représente la circulation transfrontalière des données. Il convient peut-être ici de rappeler à tous qu'une fois que des données ont quitté le Canada, le contrôle définitif de ces données relève des autorités qui les détiennent; les données sont assujetties aux lois du pays étranger et leur accès relève de ces lois. C'est pourquoi l'Union européenne (UE) a publié la Directive 95/46 sur la protection des renseignements personnels, qui demande aux commissaires à la protection des données de l'UE de cesser l'échange des données avec les pays étrangers qui n'ont pas de mesures de protection « adéquates ». Par mesures de protection adéquates, on entend non seulement une loi sur la protection des données, mais également des autorités de protection des renseignements personnels qui offrent un recours aux citoyens.

Cette question n'est pas nouvelle pour ceux qui s'intéressent à la protection des données; les dispositions de la Directive 95/46 ont causé tout un remous dans les années 1990, lorsque cette dernière a été instaurée. Quinze ans plus tard, nous en sommes encore à chercher des solutions aux différends qui résultent de la circulation mondiale des données. La commissaire à la protection de la vie privée du Canada a

aviser la personne concernée de la communication imminente des renseignements. Toutefois, c'est au responsable de l'institution que revient la décision de communiquer l'information pour des raisons d'intérêt public et de déterminer la quantité de renseignements à communiquer. La commission a la protection de la vie privée n'a pas le pouvoir d'empêcher la communication.

Les dispositions de la *Loi sur la protection des renseignements personnels* relatives à la communication de renseignements pour des raisons d'intérêt public sont donc très claires. Malheureusement, ces dispositions ne sont pas bien comprises, et, à l'occasion, la Loi est perçue comme un obstacle à la sécurité qui empêcherait la communication de renseignements personnels. Trop souvent, nous entendons des représentants d'institutions gouvernementales avancer que la *Loi sur la protection des renseignements personnels* les empêche de communiquer des renseignements personnels alors qu'en réalité, le responsable de l'institution pourrait le faire pour des raisons d'intérêt public. Cette explication erronée du rôle de la Loi présente celle-ci sous un mauvais jour, ce qui est fort regrettable.

Nous comprenons que cet aspect place parfois les institutions gouvernementales dans une situation délicate. Par exemple, un journaliste couvrant un crime ou une catastrophe naturelle peut s'acharner sur le porte-parole d'une institution et tenter d'obtenir le nom d'une victime ou d'autres renseignements personnels la concernant. Le porte-parole peut choisir de pécher par excès de prudence et de ne pas communiquer ces renseignements.

Nous n'avons rien à redire quant à une telle prudence, puisque le porte-parole n'est pas habilité par la *Loi sur la protection des renseignements personnels* à communiquer des renseignements personnels pour des raisons d'intérêt public, et la décision de communiquer des renseignements ne devrait jamais être prise à la légère. Seul le responsable de l'institution ou son délégué peut décider de communiquer l'information pour des raisons d'intérêt public. Dans plusieurs cas, l'information sera communiquée ultérieurement, mais seulement lorsque le responsable de l'institution aura déterminé qu'il est approprié de le faire.

Nous sommes préoccupés par la description simpliste dont fait souvent l'objet la *Loi sur la protection des renseignements personnels* et qui la présente comme un obstacle à la communication. Dans le but de présenter une interprétation plus juste de la *Loi sur la protection des renseignements personnels*, il serait préférable que tout porte-parole d'une institution qui se retrouve face à une décision relative à la communication de renseignements personnels réponde que la décision relève non

Communication de renseignements personnels pour des raisons d'intérêt public

La protection des renseignements personnels versus la communication injustifiée est une préoccupation constante du Commissariat. Cependant, certaines situations justifient, voire nécessitent, la communication des renseignements personnels que détiennent les institutions gouvernementales, et ce, même sans le consentement de la personne concernée. À ce nombre figure la communication de renseignements personnels pour des raisons d'intérêt public.

La Loi sur la protection des renseignements personnels autorise la communication de renseignements personnels pour des « raisons d'intérêt public » dans certaines situations. L'article 8(2)(m) de la Loi autorise la « communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

- des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée;
- l'individu concerné en tirerait un avantage certain ».

On a, par exemple, invoqué cette disposition pour rendre publics certains détails concernant une personne dont la mise en liberté constitue une menace pour la collectivité.

Le responsable de l'institution détermine si l'intérêt public l'emporte sur le droit à la protection de la vie privée. L'institution doit aviser la commissaire de son intention de communiquer des renseignements personnels pour des raisons d'intérêt public. La commissaire peut faire part au responsable de ses préoccupations à l'égard de la communication demandée, et peut, si elle estime qu'il est approprié de le faire,

Dans son rapport présenté le 15 novembre 2005, M. La Forest précise que le fardeau de persuasion incombe aux tenants de la fusion des commissariats à l'information et à la protection de la vie privée, ou aux tenants de la nomination conjointe d'un seul commissaire à la tête des deux commissariats. M. La Forest conclut qu'on ne s'est pas acquitté de ce fardeau. Les modèles à un seul ou à deux commissaires comportent chacun des avantages et des inconvénients et, selon les conclusions de M. La Forest, le contexte abstrait ne permet pas de démontrer la supériorité de l'un ou de l'autre modèle. « Compte tenu des caractéristiques uniques des environnements fédéraux relatifs à l'accès à l'information et à la protection de la vie privée, mais aussi des efforts investis par les parties intéressées dans la structure actuelle, le passage au modèle à un seul commissaire aurait, selon moi, un effet préjudiciable sur les objectifs politiques de la Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques. »

des enjeux communs aux lois en matière d'accès afin d'aborder le vaste éventail de questions soulevées dans notre rapport sur la responsabilité du gouvernement en matière de protection des renseignements personnels et la réforme de la *Loi sur la protection des renseignements personnels*.

La question de la fusion

En juillet 2005, l'honorable Gérard V. La Forest, ancien juge de la Cour suprême du Canada, a été nommé conseiller spécial auprès du ministre de la Justice pour réaliser un examen indépendant sur la possibilité de fusionner les commissariats à l'information et à la protection de la vie privée. M. La Forest était également chargé du mandat d'examiner les avantages de la nomination conjointe d'un seul commissaire aux deux fonctions en maintenant les deux commissariats.

Un changement dans la structure encadrant les questions d'accès à l'information et de protection de la vie privée au niveau fédéral pourrait avoir des répercussions sous divers angles, dont la qualité de la protection du droit à la vie privée des Canadiennes et des Canadiens.

Dans la réponse officielle que nous avons fait parvenir à M. La Forest en octobre 2005, nous avons conclu que le moment n'était pas opportun pour envisager la fusion des deux commissariats. Notre conclusion faisait état d'un manque flagrant de documents spécialisés sur les avantages et les inconvénients associés au modèle « jumelé » ou au modèle fédéral actuel. Le choix d'un modèle en particulier doit reposer sur les hypothèses plutôt que sur les données historiques.

Nous faisons remarquer également qu'il importe de ne pas laisser le débat au sujet d'un nouveau cadre faisant valoir les droits relatifs à la protection de la vie privée et à l'accès à l'information au fédéral détourner l'attention d'autres préoccupations à l'égard de ces droits – notamment, la nécessité d'un cadre législatif approprié, de ressources adéquates afin de satisfaire aux obligations imposées par la loi, ainsi que le nécessité d'un large éventail d'outils et de processus visant à promouvoir une approche orientée sur la conformité aux valeurs qu'incarnent les lois en matière d'accès à l'information et de protection de la vie privée. Nous faisons valoir qu'un examen de ces lois est primordial et devrait précéder les entretiens au sujet des modèles organisationnels. La protection de la vie privée et l'accès à l'information constituent un enjeu majeur, certes, mais d'abord et avant tout en raison de leur valeur intrinsèque, et non pour la forme que prend la structure qui les encadre.

lui confère la loi destinée au secteur privé, y compris le pouvoir de recourir à la médiation et à la conciliation pour régler des plaintes, d'effectuer des recherches sur des enjeux relatifs à la protection de la vie privée, et de sensibiliser le grand public et les institutions gouvernementales à leurs droits et obligations. Les devoirs des institutions gouvernementales à l'égard de la collecte, de l'utilisation et de la communication des renseignements personnels doivent être énoncés plus clairement. D'importantes politiques relatives à la réalisation des buts énoncés dans la *Loi sur la protection des renseignements personnels* ont été élaborées par le Conseil du Trésor. Ces obligations relatives au couplage de données, à la gestion et à la sécurité de l'information gouvernementale, à l'établissement de cadres de gestion des renseignements personnels, à la tenue d'évaluations des facteurs relatifs à la vie privée (EFPV) visant les nouveaux programmes, et aux directives en matière de protection des renseignements personnels dans le cadre d'impartition de services devraient être appuyées par la Loi. Si on ne met pas le poids de la loi derrière ces politiques, celles-ci seront soumises au bon vouloir du pouvoir exécutif.

Pour accroître la responsabilité et la transparence des institutions gouvernementales à l'égard des renseignements personnels, il faut renforcer les exigences redditionnelles et attribuer aux comités parlementaires le soutien et les ressources nécessaires pour examiner les pratiques des institutions gouvernementales en matière de renseignements personnels, ainsi que le rendement de ces institutions en ce qui concerne la conformité à la *Loi sur la protection des renseignements personnels*. Les institutions doivent demeurer responsables des renseignements personnels qu'elles sont habilitées à recueillir, même si la collecte ou le traitement des données sont assurés par d'autres entités, en particulier des entrepreneurs à l'extérieur du Canada.

Bien que cette situation échappe à la période visée par le présent rapport, on ne saurait passer sous silence la *Loi fédérale sur l'imputabilité*, présentée par le nouveau gouvernement le 11 avril 2006. Ce projet de loi s'assortit d'un premier ensemble de modifications proposées à la *Loi sur l'accès à l'information* et de modifications parallèles à la *Loi sur la protection des renseignements personnels*. Ces modifications élargissent la portée des lois afin que celles-ci s'appliquent à davantage de sociétés d'État, mais aussi aux hauts fonctionnaires du Parlement (y compris le CPVP). Le gouvernement a d'ailleurs confirmé son engagement à procéder à une réforme exhaustive de la *Loi sur l'accès à l'information*, ce qui exigera nécessairement qu'on prenne en considération les dispositions parallèles de la *Loi sur la protection des renseignements personnels*. Nous espérons que c'est au cours du nouvel exercice que le gouvernement lancera enfin l'examen et la mise à jour « urgents et évitables » de la *Loi sur la protection des renseignements personnels* et que cette réforme ira au-delà

responsabilisation, et nous espérons que l'examen et la modification de la *Loi sur la protection des renseignements personnels* qui s'imposent auront enfin lieu. Dans le cadre de la préparation de notre rapport sur la responsabilité du gouvernement en matière de protection des renseignements personnels, nous avons pris connaissance des réformes proposées au Comité par le commissaire à l'information en septembre 2005 et du rapport que le conseiller spécial auprès du ministre de la Justice, M. Gérard La Forest, a présenté en novembre.

Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* il y a plus de 20 ans, le contexte de la protection de la vie privée est devenu beaucoup plus complexe. Les changements technologiques et sociaux survenus au cours des 20 dernières années – comme la création d'Internet et du World Wide Web, les nouvelles technologies de l'information et de la communication, la mondialisation, les systèmes mondiaux de signalisation, la vidéosurveillance, l'impartition, l'extraction de données et la marchandisation des renseignements personnels – n'ont pas simplement changé le paysage qui nous entoure; ils nous ont carrément transportés sur une autre planète.

À titre de loi quasi constitutionnelle, la *Loi sur la protection des renseignements personnels* doit avoir préséance sur d'autres lois, sauf dans certains cas très exceptionnels. Toutes les institutions gouvernementales fédérales doivent être visées par la *Loi sur la protection des renseignements personnels* : celle-ci ne saurait s'appliquer uniquement aux ministères et aux organismes. Les hauts fonctionnaires du Parlement, les sociétés d'État, les diverses fondations établies au cours des dernières années et les autres entités exerçant des fonctions importantes liées à la santé et à la sécurité publique doivent également se plier aux exigences de la *Loi sur la protection des renseignements personnels*. Toute personne, même n'étant pas citoyenne canadienne ou présente en territoire canadien, doit jouir du droit de demander accès aux renseignements personnels la concernant que détiennent une institution gouvernementale canadienne. La définition de « renseignements personnels » doit, à une époque où les réalités technologiques et numériques permettent d'assurer une surveillance en temps réel, comprendre les renseignements enregistrés et non enregistrés au sujet d'une personne identifiable. De plus, une personne doit avoir la possibilité de contester devant les tribunaux non seulement un refus d'accès à ses renseignements personnels, mais aussi la collecte, l'utilisation ou la communication inappropriée de ces renseignements.

La *Loi sur la protection des renseignements personnels* doit conférer à la commissaire à la protection de la vie privée un mandat au moins aussi vaste que celui que

recommandations formulées par le commissaire à la protection de la vie privée au cours des années 90. Il avait déclaré que les lacunes de la *Loi sur la protection des renseignements personnels* étaient :

« [...] encore plus évidentes depuis l'adoption par le Parlement de la *Loi sur la protection des renseignements personnels* et les *documents électroniques*. Cette Loi (qui réglemente le traitement des renseignements personnels dans le secteur privé) comprend beaucoup de caractéristiques supérieures à la *Loi sur la protection des renseignements personnels*, ce qui rend l'examen exhaustif de cette dernière à la fois urgent et inévitable. »

Un examen détaillé de la Loi, intitulé *Réforme de la Loi sur la protection des renseignements personnels : Détermination et examen des questions*, a été élaboré par le Commissariat en décembre 1999, diffusé en juin 2000 et présenté au ministre de la Justice en vue de cet examen « urgent et inévitable ».

Cet examen n'a toujours pas eu lieu.

Les Canadiennes et les Canadiens sont beaucoup plus au fait des principes de protection des renseignements personnels qui sous-tendent la loi visant le secteur privé; ils attendent sans aucun doute à ce que les renseignements personnels qu'ils détiennent le gouvernement bénéficient d'une protection au moins égale à la protection des renseignements personnels confiés aux entreprises. Si l'examen de la Loi était « à la fois urgent et inévitable » en 2000, il l'est d'autant plus aujourd'hui.

À cette fin, le tout dernier rapport produit par le Commissariat met l'accent sur les obligations des institutions gouvernementales. Ce rapport a été produit sur l'invitation du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, invitation renouvelée à l'occasion de la comparution du CPVP devant le Comité, l'automne dernier, pour discuter de nos rapports annuels pour l'exercice 2004-2005. Ce rapport, qui porte sur la responsabilité du gouvernement en matière de protection des renseignements personnels et la réforme de la *Loi sur la protection des renseignements personnels*, a été présenté au comité récemment.

La *Loi sur la protection des renseignements personnels* devait accompagner la *Loi sur l'accès à l'information*; elle devrait, dans la mesure du possible, continuer de jouer ce rôle. Le nouveau gouvernement articule son mandat autour de la notion de

L'un des principaux comités liés aux fonctions du Commissariat est le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. L'importance de ce comité relativement nouveau (établi à la fin de 2004) est considérable : la population canadienne dispose maintenant d'un comité permanent de la Chambre des communes voué aux questions se rapportant à la protection de la vie privée. La commissaire à la protection de la vie privée du Canada et d'autres représentants du CPVP ont comparu à trois reprises devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique en 2005-2006. Si ces comparutions avaient pour but, entre autres, de répondre à des questions concernant nos activités dans le cadre de l'examen de notre budget et de nos rapports annuels, les députés membres du Comité ont également soulevé de nombreuses questions et fait part de leurs préoccupations relatives aux principaux défis et possibilités en matière de protection de la vie privée au Canada. Le CPVP compte maintenant la relation de travail constructive qu'il entretenait avec ce comité au cours de la 39^e législature. Les enjeux liés à la protection de la vie privée ne cessent de se multiplier et de gagner en complexité. Il s'avère donc crucial que le Parlement soit doté d'un mécanisme permettant d'examiner ces enjeux et de se pencher sur les préoccupations des Canadiennes et des Canadiens.

Enfin, un nouveau Groupe consultatif de la Chambre sur le financement des hauts fonctionnaires du Parlement a été créé cette année. Ce groupe a été chargé d'évaluer la demande de ressources additionnelles que le CPVP a présentée et de faire des recommandations à cet égard. Le CPVP a comparu à deux reprises devant ce groupe pour présenter son analyse de rentabilisation.

Réforme de la Loi sur la protection des renseignements personnels

Les premières recommandations destinées à la réforme de la Loi sur la protection des renseignements personnels remontent au tout premier examen exigé par la Loi, lequel a mené, en 1987, à la publication du rapport du Comité permanent de la justice et du solliciteur général intitulé *Une question à deux volés : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*. Le rapport, qui contenait plus de 100 recommandations, a reçu l'appui unanime des membres du Comité, mais aucun des changements recommandés n'a été apporté; pourtant, dans sa réponse, le gouvernement s'était engagé à apporter des changements au plus tard à l'automne 1988.

Dans son dernier rapport, pour l'exercice 1999-2000, l'ancien commissaire Bruce Phillips avait signalé que le Parlement ne s'était pas penché sur la Loi sur la protection des renseignements personnels depuis 14 ans, et ce, malgré les nombreuses

d'une combinaison d'alcool et de drogue, ainsi qu'à prélever des échantillons de substances corporelles aux fins d'analyse pour déceler la présence d'une drogue ou d'une combinaison d'alcool et de drogue chez une personne. Le CPVP a exprimé son appui à l'intention de cette loi, dont l'objet est d'accroître la sécurité des routes et de protéger les Canadiennes et les Canadiens des conséquences de la conduite avec facultés affaiblies. Cependant, certaines préoccupations demeurent quant à la façon dont le projet de loi propose d'aborder le problème. Plus particulièrement, nos préoccupations ont trait à l'efficacité et à la proportionnalité des mesures proposées. Selon l'un des principes fondamentaux en matière de traitement équitable des renseignements personnels qui sous-tendent la Loi, les renseignements personnels ne doivent pas être recueillis à moins que ceux-ci soient utilisés aux fins particulières pour lesquelles ils sont recueillis. Contraindre des personnes à fournir des substances corporelles est une atteinte à la vie privée. L'atteinte est d'autant plus sérieuse lorsque les échantillons ne permettent pas avec certitude de mesurer l'affaiblissement des facultés. Nous avons néanmoins fait valoir que si le gouvernement décidait d'adopter la Loi en dépit de ces préoccupations, il lui faudrait prévoir d'autres dispositions pour garantir que les substances corporelles recueillies et les résultats des tests soient adéquatement protégés. Le projet de loi C-16 est mort au Feuilleton à l'étape de rapport du Comité.

- Examen de la *Loi antiterroriste*. (Devant le Comité spécial du Sénat sur la *Loi antiterroriste* et le Sous-comité de la Chambre des communes sur la sécurité publique et nationale.)

La *Loi antiterroriste* a reçu la sanction royale le 18 décembre 2001. Cette loi est venue modifier le *Code criminel*, la *Loi sur les secrets officiels*, la *Loi sur la preuve au Canada*, la *Loi sur le recyclage des produits de la criminalité* et d'autres lois, et a édité la *Loi sur l'enregistrement des organismes de bienfaisance* (*renseignements de sécurité*), en vue de lutter contre le terrorisme. En 2005, un comité de la Chambre et un comité du Sénat ont mené, de façon indépendante, un examen détaillé de la *Loi antiterroriste*, selon lequel la Loi doit faire l'objet d'un examen dans les trois ans qui suivent sa promulgation. Le Commissariat à la protection de la vie privée du Canada a comparu devant les deux comités qui procédaient à l'examen. Nos observations portaient principalement sur le manque de faits et d'éléments de preuve justifiant les mesures prévues par la *Loi antiterroriste*. Nous avons exhorté les comités à évaluer de manière critique la question de la proportionnalité et à prendre en considération plusieurs de nos recommandations pratiques pour aborder la question des répercussions cumulatives des mesures antiterroristes sur le droit à la protection de la vie privée des Canadiennes et des Canadiens.

des données du recensement puissent être communiquées 92 ans après la collecte. Le CPVP ne s'oppose pas à la communication des données après cette période, mais souhaite que des dispositions en matière de consentement soient ajoutées à la Loi, de façon à ce que celle-ci prévienne l'accès aux Canadiennes et aux Canadiens le droit de décider eux-mêmes si leurs données personnelles recueillies au moment d'un recensement seront un jour rendues disponibles au grand public. Le projet de loi a reçu la sanction royale le 29 juin 2005.

- *Projet de loi C-37, Loi modifiant la Loi sur les télécommunications.* (Devant le Comité permanent de l'industrie, des ressources naturelles, des sciences et de la technologie de la Chambre des communes.)

Ce projet de loi vise à réduire le nombre d'appels de télémarketing que les Canadiennes et les Canadiens reçoivent à la maison en donnant au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) la capacité d'établir une liste de numéros de téléphone exclus (LNTF) à l'échelle nationale. Selon la nouvelle loi, le CRTC a le pouvoir d'imposer des pénalités sévères aux télévendeurs qui ne respectent pas les règles. Le CPVP a appuyé fortement l'esprit général du projet de loi au moment de sa première lecture au Parlement. Cependant, le projet de loi C-37 comporte également une liste de télévendeurs qui ne sont pas assujettis aux exigences du CRTC ni à la liste des interdictions liées à la LNTF. Le CPVP s'est opposé ouvertement à l'inclusion de ces exceptions dans le projet de loi. Nous avons alors suggéré à la Chambre des communes de reporter l'ajout de toute exclusion à une date ultérieure et que le Parlement mène d'abord des consultations intensives à cet égard auprès des Canadiennes et des Canadiens, comme l'avait recommandé le ministre responsable du projet de loi à ce moment-là. Le projet de loi C-37 a reçu la sanction royale le 25 novembre 2005; il aura force de loi à une date qui sera fixée par un décret de la gouverneure en conseil.

- *Projet de loi C-16, Loi modifiant le Code criminel (conduite avec facultés affaiblies) et d'autres lois en conséquence.* (Devant le Comité permanent de la justice, des droits de la personne, de la sécurité publique et de la protection civile de la Chambre des communes.)

Ce projet de loi modifie le *Code criminel* afin de préciser que la mention « conduite d'un véhicule sous l'effet de l'alcool ou d'une drogue », à l'alinéa 253(1)(a) inclut la conduite sous l'effet d'une combinaison d'alcool et de drogue. Le projet de loi autorise des agents de la paix ayant suivi une formation spéciale à effectuer des tests afin de déterminer si une personne est affaiblie par l'effet d'une drogue ou

Activités parlementaires : bilan annuel

En ce qui concerne l'activité parlementaire, l'exercice 2005-2006 s'est révélé très chargé pour le Commissariat à la protection de la vie privée (CVP). L'un des aspects principaux de notre travail consiste à comparaître devant les comités du Sénat et de la Chambre des communes en vue de prodiguer des conseils d'experts sur l'incidence sur la protection de la vie privée de projets de loi et d'autres questions de politiques envisagées par le Parlement.

Le Commissariat a été invité à comparaître devant les comités parlementaires à 11 reprises au cours de l'exercice 2005-2006 (16 comparutions au cours de l'année civile 2005). Ces comparutions représentent beaucoup de travail pour un organisme de notre mandat, puisque la commissaire à la protection de la vie privée est une haute fonctionnaire du Parlement. Dix de ces onze comparutions portaient sur des projets de loi et des enjeux en matière de politiques qui sont du ressort de la *Loi sur la protection des renseignements personnels*, même si certaines comparutions, comme celles liées au financement, se rapportaient aussi à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Le projet de loi S-18, *Loi modifiant la Loi sur la statistique*. (Devant le Comité permanent de l'industrie, des ressources naturelles, des sciences et de la technologie de la Chambre des communes.)

- L'adoption de cette loi élimine une ambiguïté juridique relative à l'accès aux données du recensement recueillies entre 1910 et 2005. La Loi permet un accès non limité à ces données 92 ans après leur collecte. À compter de 2006, le consentement des Canadiennes et des Canadiens est requis pour que

- effectuer des recherches sur les nouvelles tendances et les nouveaux enjeux relatifs à la protection de la vie privée afin d'aider les citoyens et les décideurs à mieux comprendre les défis d'aujourd'hui et de demain dans cette sphère;
- initier des projets de sensibilisation du grand public visant à mieux informer les personnes de leurs droits et à mieux informer les institutions et les organisations de leurs obligations;
- utiliser un processus d'enquête simplifié pour s'attaquer à l'arriéré des plaintes;
- soutenir les efforts de renouvellement institutionnel.

Analyse de rentabilisation : ressources

L'an dernier, le Commissariat a pris part avec enthousiasme à un processus innovateur et entièrement nouveau pour l'approbation de financement pour les activités des hauts fonctionnaires du Parlement. Nous avons accueilli très favorablement cette occasion d'engager un dialogue constructif avec le Parlement sur nos besoins financiers. Mais auparavant, nous nous sommes bien préparés. Notre Vision et plan de services institutionnel et notre analyse de rentabilisation en vue d'un financement permanent constituent un cadre solide pour garantir le droit à la protection de la vie privée de la population canadienne et des résidents du Canada, ainsi que pour répondre aux besoins du Parlement, à titre de spécialistes de la protection de la vie privée, au cours de l'examen des dispositions législatives en la matière. Le plan de services et l'analyse de rentabilisation constituent la base sur laquelle s'appuie le Commissariat pour jouer son rôle avec plus de force et d'efficacité.

Cette vision a été approuvée par les parlementaires. Le nouveau Groupe consultatif de la Chambre des communes sur le financement des hauts fonctionnaires du Parlement nous a également fortement appuyés. Le Commissariat sera désormais plus apte à servir les intérêts des Canadiennes et des Canadiens grâce à une augmentation de près de 50 % des ressources humaines et financières. En fin d'exercice pour l'année fiscale 2005-2006, soit la période couverte par ce rapport, nos prévisions tenaient compte de cette augmentation au cours des deux prochaines années.

- mener un nombre significatif de vérifications et d'examen pour promouvoir une plus grande conformité et contribuer à l'élaboration d'un solide cadre de gestion des renseignements personnels;
 - travailler en collaboration avec les institutions gouvernementales et effectuer des analyses de nature juridique et politique de lois et de projets de loi afin d'appuyer le Parlement dans ses travaux;
 - avoir recours, de façon plus proactive, efficace et importante, aux outils d'application de la loi que lui a confiés le Parlement, comme les plaintes émanant de la commissaire, les poursuites en justice et la communication d'information d'intérêt public;
- LPRPDE :*
- conformément à la Loi sur la protection des renseignements personnels et à la Dote de fonds adéquats, le Commissariat pourra effectuer les activités suivantes,

Le Commissariat a procédé à deux importantes analyses : le document Vision et plan de services institutionnel ainsi que l'analyse de rentabilité en vue d'un financement permanent. Ces deux documents définissent notre rôle tel qu'il doit être, en tant que représentant du Parlement au service des intérêts des Canadiennes et des Canadiens, et ce dont nous avons besoin pour atteindre nos objectifs.

Vision du Commissariat à la protection de la vie privée du Canada

Nous privilégions l'embauche de nouveaux talents et le recrutement de personnes hautement qualifiées. Nous avons mené à terme un ambitieux programme qui visait à corriger toutes les lacunes au sein de la direction de l'organisme. Jusqu'à ce jour, les vérifications et les évaluations du Commissariat effectuées par le Bureau du vérificateur général du Canada, la Commission de la fonction publique ainsi que par la Commission canadienne des droits de la personne ont été positives. Nous avons aussi mis en œuvre un processus réfléchi et systématique pour déterminer nos besoins organisationnels. Le Commissariat est une institution stable et mérite la confiance du Parlement et de la population canadienne dont il sert les intérêts.

Il est maintenant temps d'instaurer la nouvelle vision du Commissariat, ce qui les façons de faire du Commissariat. Celui-ci se retrouve engagé sur la bonne voie. chose malheureuse est bon : les difficultés nous ont permis de revoir de fond en comble Les dernières années ont été épuisantes pour le Commissariat. Mais à quelque

répondre aux urgences, plutôt que de prévoir et de composer efficacement avec tout nouveau problème relatif à la protection de la vie privée.

UN MANDAT RENFORCÉ

Lincombe au Commissariat de surveiller la conformité à la Loi sur la protection des renseignements personnels et à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Bien que ces deux lois soient distinctes, les ressources qui y sont affectées ne le sont pas. À ce jour, le

Commissariat n'a pas reçu de financement permanent lui permettant d'assumer ses fonctions en vertu de la LPRPDE, et le financement affecté à la Loi sur la protection des renseignements personnels est demeuré inchangé depuis plusieurs années. Trois années seulement ont été octroyées au financement de la LPRPDE. La LPRPDE, dont l'application s'est échelonnée sur plusieurs étapes, est entrée en vigueur en 2001 et a atteint sa pleine mise en œuvre en 2004. Il nous semblait important de laisser retomber la poussière avant de définir nos besoins financiers à long terme. La LPRPDE est pleinement en vigueur depuis maintenant deux ans, et les demandes qui nous sont adressées en vertu des deux lois sont de plus en plus nombreuses.

Le financement destiné à l'application des deux lois, ne nous permettait pas de répondre aux exigences d'un mandat aux multiples facettes. Conséquemment, nous devons composer avec un arriéré considérable de plaintes à traiter, en particulier les plaintes relevant de la Loi sur la protection des renseignements personnels, les personnes qui ont déposé ces plaintes commencent à s'impatienter, ce que nous comprenons sans peine. L'équipe des vérificateurs est trop réduite pour nous permettre d'effectuer des vérifications efficaces en vue d'assurer la conformité. Bien que nous ayons mis en place une approche axée sur la gestion du risque, il nous faut intensifier nos activités de vérification. De plus, en raison des restrictions financières, notre stratégie de communication est essentiellement réactive, alors que c'est d'une stratégie proactive de sensibilisation du grand public sur les droits et les obligations en matière de protection de la vie privée dont nous avons besoin. Pour leur part, la Direction de la recherche et des politiques ainsi que la Direction des services juridiques, ont dû se limiter à

de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, nos recommandations pour modifier la *Loi sur la protection des renseignements personnels*, et voyons d'un œil favorable la perspective d'un dialogue utile et fructueux.

Depuis ma nomination au poste de commissaire à la protection de la vie privée en décembre 2003, et sans aucun doute au cours du dernier exercice, mon équipe et moi avons concentré nos efforts à la poursuite du renouvellement institutionnel du Commissariat. Remettre le Commissariat sur pied se devait d'être une priorité. Nous avons également consacré nos efforts, l'année dernière, à une analyse de rentabilisation en vue d'obtenir du financement stable et à long terme; le processus faisait appel à un examen indépendant de nos activités ainsi qu'à une présentation devant un Groupe consultatif spécial du Parlement afin que ce dernier élabore ses recommandations. Il me fait plaisir d'annoncer que le Commissariat entame un nouveau chapitre. Nous allons maintenant de l'avant avec un regain de vigueur. Nous continuerons de travailler en collaboration avec nos homologues provinciaux et territoriaux, ainsi qu'avec nos collègues à l'échelle internationale, afin de relever les importants défis en matière de protection de la vie privée qui se dessinent à l'horizon.

des renseignements personnels. Une loi qui, tiendra compte des réalités à l'ère de l'information, des défis que pose l'ubiquité numérique, et des imposants systèmes gouvernementaux dont la capacité de surveillance actuelle était inimaginable en 1982. Les résultats d'un sondage révèlent que plus de 70 % de la population canadienne estime que la protection à la vie privée et la protection des renseignements personnels se sont grandement dégradées; tout indique que la protection de la vie privée figure parmi les enjeux les plus importants auxquels le pays est confronté.

La population canadienne mérite d'obtenir concrètement réparation pour les torts qui lui sont causés, ce que ne peut lui procurer une commissaire à la protection de la vie privée dépourvue même du pouvoir de s'adresser à la Cour fédérale en vue d'obtenir jugement et dommages-intérêts pour collecte injustifiée ou communication malveillante de renseignements personnels. En 1982, nous avons ouvert la voie pour garantir certains droits aux Canadiennes et aux Canadiens, nous sommes allés plus loin en ce sens avec l'entrée en vigueur, en 2001, de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* visant le secteur privé. Nous devons maintenant continuer dans cette direction en demandant au gouvernement de satisfaire aux normes nécessaires à l'ère de l'information. Il est inacceptable que les normes de protection de la vie privée soient plus sévères pour le secteur privé qu'elles ne le sont pour le secteur public.

À l'automne 2007, nous aurons l'honneur d'être les hôtes de la Conférence internationale des commissaires à la protection des données et de la vie privée, qui se déroulera à Montréal. Les pays étrangers, dont plusieurs participeront à cet événement important, tiennent de plus en plus le Canada pour modèle en matière de protection des données. À titre d'exemple de l'intérêt des pays étrangers à l'endroit de notre cadre de protection des données, nous nous sommes engagés dans des activités de développement professionnel avec les autorités désignées du Mexique, de la France et du Royaume-Uni. Le Canada doit demeurer un chef de file dans ce domaine et, à mon avis, il y contribuera essentiellement par la mise à jour de la loi couvrant le secteur public. Il n'est tout simplement pas admissible que les normes de protection de la vie privée soient plus sévères pour le secteur privé.

Une véritable protection de la vie privée exige un équilibre des pouvoirs entre le citoyen et l'État, incluant une surveillance des activités de l'État et un pouvoir efficace d'intervention. Nous sommes aptes à mener à bien cette entreprise; nous envisageons avec impatience d'entreprendre les fonctions qui en découleraient. Engagés dans cette cause, nous avons présenté très récemment au Comité permanent

(CPVP) a été établi, c'était un organisme de petite envergure doté de pouvoirs limites; le Secrétaire du Conseil du Trésor et le ministre de la Justice étaient chargés de mettre en œuvre la nouvelle loi et de prêter leur soutien aux fonctionnaires pour interpréter celle-ci.

Aujourd'hui, notre capacité à comprendre le monde et à emboîter le pas aux changements technologiques est confrontée aux nouveaux défis en matière de sécurité et de risques qu'entraîne la possibilité illimitée de stockage de données, de transmission de données et de forage de données. Nous sommes limités par notre capacité restreinte à comprendre et à imaginer les conséquences de la circulation et de l'agrégation des données, et par nos aptitudes limitées à informer le grand public. La protection des données constitue un défi d'envergure mondiale aujourd'hui, une action menée dans une région éloignée du monde peut avoir des répercussions directes sur la protection de la vie privée des Canadiennes et des Canadiens. Ainsi, un expéditeur de courriels en masse véhicule des pourriels et des logiciels espions peut semer le chaos chez un fournisseur canadien de services Internet même s'il est envoyé de l'Europe de l'Est; on procède actuellement à la mise à l'écoute de voies de communications – ce qui permet de décoder, entre autres, des activités de terrorisme ou de blanchiment d'argent – dont la portée et l'application s'étendent à l'échelle mondiale; les voyageurs canadiens doivent posséder pièces d'identité et instruments financiers pour justifier leur crédibilité dans leurs activités commerciales outre-frontières. Aujourd'hui, la vie est complexe; la protection de la vie privée l'est également.

Il nous faut comprendre les conséquences des innombrables nouveaux systèmes d'information, des nouvelles lois et réglementations, des nouveaux systèmes de surveillance conçus au nom de la sécurité publique. Nous devons procéder à la vérification d'un plus grand nombre de ces mesures afin d'informer plus rapidement les ministères et de leur prêter assistance. Car, bien qu'ils doivent prendre moult de décisions complexes, les ministères ne maîtrisent pas nécessairement aussi bien que nous les enjeux en matière de protection de la vie privée. Nous sommes déterminés à progresser grâce à des ressources additionnelles, et à constamment perfectionner notre capacité à fournir conseils et assistance à la population canadienne, au Parlement et aux fonctionnaires qui travaillent à améliorer la qualité de vie des Canadiennes et des Canadiens.

Au risque de ressembler à Oliver Twist, j'ai envie de dire : « J'en voudrais encore, monsieur, s'il vous plaît. » J'entretiens l'espoir que nous puissions célébrer l'anniversaire de la Loi visant le secteur public fédéral, avec la conviction que le Parlement nous présentera prochainement une nouvelle *Loi sur la protection*

7

l'année 2007 marquera le 25^e anniversaire de la Loi sur la protection des renseignements personnels, la toute première loi exhaustive en matière de

protection de la vie privée au Canada. Issue de la révision de la quatrième partie (1977) de la Loi canadienne sur les droits de la personne – qui tenait compte des principes fondamentaux et instaurait le rôle de commissaire à la

protection de la vie privée à titre de membre de la Commission canadienne des

droits de la personne –, la Loi sur la protection des renseignements personnels s'ancrait dans la conception générale que l'on avait du gouvernement dans les années 60 et 70. On se préoccupait alors des vastes bases de données centralisées qui fonctionnaient à l'aide de gros ordinateurs. Il était question de fichiers et l'image que nous nous faisons d'un système de gestion des dossiers était un classeur rempli de documents papier. Cette époque précédait l'arrivée des ordinateurs personnels, d'Internet et des puissants moteurs de recherche tel Google. Les fonctionnaires travaillaient sur papier; ils dactylographiaient les formulaires en triplicata.

Pourquoi, me demanderez-vous, ce retour en arrière? Parce que le monde a subi des changements en profondeur, des changements grandement inquiétants du point de vue de la protection de la vie privée et des droits de la personne. À l'époque où nous concevions de puissants ordinateurs centraux qui, armés du nouveau numéro d'assurance sociale pour coupler les données avec une certaine fiabilité, avaient une incidence réelle sur la protection de la vie privée, le monde dans lequel nous vivions était inévitablement limité dans ses capacités : capacité limitée de stockage de données, capacité limitée de couplage de données, capacité limitée à faire circuler les données et, par conséquent, à exposer la population aux risques d'atteintes à la protection de la vie privée. Lorsque le Commissariat à la protection de la vie privée



Vérification et examen	57
Nécessité d'un cadre de gestion de la protection de la vie privée plus rigoureux	58
Contrôle et responsabilisation accrues en matière de circulation transfrontalière	
des données	61
Nos principales conclusions	63
Importance des évaluations des facteurs relatifs à la vie privée (EFFVP)	65
Autres activités	70
Devant les tribunaux	73
Demandaes adressées en vertu de la Loi sur la protection des renseignements personnels	73
Le contrôle judiciaire	74
Sensibilisation du grand public et communications	77
Les sondages d'opinion	77
Discours et événements spéciaux	78
Les relations avec les médias	78
Le site Web	79
Les publications	79
Les communications internes	79
Les Services de gestion intégrée	81
Planification et reddition des comptes	81
Les ressources humaines	81
Finances et administration	83
Gestion et technologie de l'information	83
Nos besoins en ressources	83
Information financière	83
Annexe 1	85
Annexe 2	89

TABLE DES MATIÈRES

Avant-propos.....	1
Un mandat renforcé.....	5
Point de vue de la politique.....	9
Activités parlementaires : bilan annuel.....	9
Réforme de la Loi sur la protection des renseignements personnels.....	12
La question de la fusion.....	16
Enjeux en matière de politiques.....	19
Communication de renseignements personnels pour des raisons d'intérêt public.....	19
Circulation transfrontalière des données.....	21
Relations internationales.....	23
Appareils d'identification par radiofréquence (AIRF).....	24
Lignes directrices en matière de vidéosurveillance.....	24
Gestion de l'identité et lutte contre le crime et la terreur.....	24
Plaintes.....	29
Définition des types de plaintes.....	29
Définitions des conclusions et d'autres dispositions en vertu de la Loi sur la protection des renseignements personnels.....	35
Conclusions selon le type de plainte.....	36
Durée de traitement des enquêtes faisant suite à des plaintes – Loi sur la protection des renseignements personnels.....	39
Cas choisis – Loi sur la protection des renseignements personnels.....	40
Incidents en vertu de la Loi sur la protection des renseignements personnels.....	46
Communiqués d'intérêt public en vertu de la Loi sur la protection des renseignements personnels.....	50
Processus d'enquête en vertu de la Loi sur la protection des renseignements personnels.....	52
Demandes de renseignements.....	54

**Commissionnaire à la protection
de la vie privée du Canada
of Canada Privacy Commissioner**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél : (613) 995-8210
Télécc : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tél : (613) 995-8210
Fax : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



juin 2006

L'honorable Peter Milliken, député
Président
Chambre des communes
Ottawa
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1er avril 2005 au 31 mars 2006 conformément à la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

Jennifer Stoddart

Jennifer Stoddart
Commissionnaire à la protection
de la vie privée du Canada



Juin 2006

L'honorable Noël A. Kinsella, sénateur
Président
Sénat du Canada
Ottawa
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2005 au 31 mars 2006 conformément à la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

Suzanne Stodart
Jennifer Stodart
Commissaire à la protection
de la vie privée du Canada

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

Téléphone : (613) 995-8210
1 800 282-1376
Télec.: (613) 947-6850
ATS (613) 992-9190

© Ministère des Travaux publics et Services gouvernementaux Canada 2006
No de cat. IP50-2006
0-662-49235-8

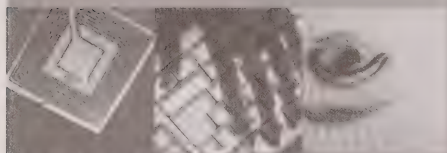
Cette publication est également disponible sur notre site Web à www.privcom.gc.ca.

Canada

RAPPORT CONCERNANT LA
Loi sur la protection des
renseignements personnels



Rapport annuel au Parlement 2005-2006

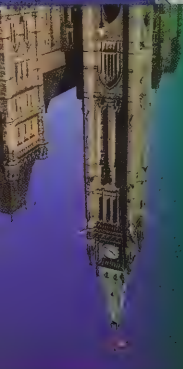


Privacy Commissioner
of Canada



Commissioner de la vie privée du Canada

RAPPORT CONCERNANT LA
Loi sur la protection des
renseignements personnels



Rapport annuel au Parlement 2005-2006

Vie privée





Office of the
Privacy Commissioner
of Canada

CA1
PC
-A573

Gov't Publications

Privacy

ANNUAL REPORT TO PARLIAMENT

2007-2008

Report on the *Privacy Act*





Office of the
Privacy Commissioner
of Canada



Privacy

ANNUAL REPORT TO PARLIAMENT

2007-2008

Report on the *Privacy Act*



Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2008
Cat. No. IP50-2008
ISBN 978-0-662-05790-1

This publication is also available on our website at www.privcom.gc.ca.

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



December 2008

The Honourable Noël A. Kinsella, Senator
The Speaker
The Senate of Canada
Ottawa, Ontario K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2007 to March 31, 2008.

Sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tél.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



December 2008

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2007 to March 31, 2008.

Sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

Message from the Commissioner.....1

Key Accomplishments in 2007-2008.....9

Privacy by the Numbers 13

Passport Canada Audit: *Significant Risk for Privacy*..... 15

Administrative and Quasi-judicial Bodies:

Balancing Openness and Privacy in the Internet Age 23

Privacy Training in the Federal Public Service:

The Need for a Comprehensive Approach..... 33

Update on *Privacy Act* Reform: *First Steps Toward a Legislative Overhaul* 41

Proactively Supporting Parliament 51

 Law Enforcement and National Security Initiatives 51

 Other Legislation and Initiatives with an Impact on Privacy 57

Responding to Complaints and Privacy Incidents 59

Other OPC Activities..... 77

 Audit and Review 77

 In the Courts 84

 Access to Information and Privacy Unit 86

 International Conference 87

The Year Ahead..... 89

Appendix 1 91
Definitions of Complaint Types 91
Definitions of Findings and other Dispositions under the *Privacy Act* 92

Appendix 2 94
Investigation Process under the *Privacy Act*. 94

Appendix 3 96
Privacy Act Inquiry and Investigation Statistics. 96
Inquiries Statistics 96
Complaints Received by Type 97
Top 10 Institutions by Complaints Received 97
Complaints Received by Institution 98
Complaints Received by Province/Territory 99
Closed Complaints by Finding 100
Findings by Complaint Type 100
 Complaints (All Types) Closed 100
 Access and Privacy Complaints Closed 101
 Time Limits Complaints Closed 101
Time Limits Closed by Institution and Finding 102
Access and Privacy Complaints Closed by Institution and Finding 103
Complaint Investigations Treatment Times 105
 By Finding. 105
 By Complaint Type 105



MESSAGE FROM THE COMMISSIONER

The doors of the Office of the Privacy Commissioner of Canada opened for business 25 years ago.

Canada's first Privacy Commissioner, John Grace, summarized the deep significance of his new mandate to protect the privacy of Canadians in his first annual report:

Societies which treat privacy with contempt and use personal information as a cheap commodity will sooner or later hold the same attitudes towards their citizens. Privacy, therefore, is not simply a precious and often irreplaceable human resource; respect for privacy is the acknowledgement of respect for human dignity and of the individuality of man.

The source for a concern with privacy is an innate respect for personhood. Privacy is the ultimate minority protection. That is why the claim of privacy is so much more than a cry to be left alone or a fashionable obsession.

A quarter-century later, those eloquent words remain as true as ever. Privacy continues to be a deeply held value. However, it is also an increasingly fragile value.

Even that first annual report observed “it has become trite to say that personal privacy is threatened as never before in human history.... The confluence of new technologies with ever-insistent claims of the state to know, to be efficient, or both, has changed the quantitative and qualitative nature of the problem.”

Since then, the power of computers has multiplied many times over.

So too have governments' appetites for personal information about their citizens. In Canada and elsewhere, the rationale of safety and national security has been used to justify a dramatic expansion in the amount of personal information governments collect, analyze and share about us.

The potent combination of state interest in personal information and technological advances making it possible to gather and exploit this data on a massive scale is a theme highlighted – once again – in this 2007-2008 annual report on Canada's public sector privacy law. (Our work related to private sector organizations is described in our annual reports on the *Personal Information Protection and Electronic Documents Act*, or PIPEDA.)

New Threats to a Fragile Value

This year, for example, our Office, along with our provincial and territorial counterparts, sounded the alarm about Canada's Passenger Protect program – also known as the no-fly list – and the secretive use of personal information to determine who may and may not board aircrafts. The program raises profound concerns about privacy and other rights, such as mobility, access to information and due process – yet we have seen no evidence demonstrating the effectiveness of no-fly lists.

We also pointed out potential privacy and security risks related to the development of enhanced driver's licences as an alternative to the Canadian passport.

Our Office, along with our counterparts in every other provincial and territorial office responsible for privacy protection, have concerns about the personal information of participating drivers leaving Canada and the potential that RFID chips in the licences could permit surreptitious location tracking. We also have concerns about our inability, in practice, to oversee how U.S. authorities receive and use this information.

Both the no-fly list and enhanced driver's licences are well-intentioned initiatives – one is aimed at preventing terrorist incidents on planes; the other at providing Canadians with an alternative form of identification for crossing the Canada-U.S. border.

We are *not* arguing that the government has any malicious or intrusive intentions, even as it develops programs that result in increased surveillance of Canadians.

However, there needs to be a greater acknowledgement of the fact that our privacy rights are fragile in the face of government. They falter each time we trade away the personal and private for promises of more safety, greater efficiency or faster service.

There must also be a wider recognition of the reality that with each well-intentioned promise comes an increased erosion of privacy, risk of data security, diminished intellectual freedom and less personal autonomy.

The Orwellian dystopia was predicated on a totalitarian society. In our democracy, benevolent intentions appear to be pushing us toward a surveillance society.

Building Respect for Privacy Rights

Privacy, like any other freedom, is not an absolute right. It is conditional, limited by other rights we have recognized in our laws. And it is contextual – other laws may override it. There may be some cases where privacy protections must give way to protect a greater good, be it public health, consumer safety or national security.

However, we should *only* be asked to make this sacrifice when it is clear that the promised outcome – such as safer air travel – will actually be achieved *and* that there is no other less privacy-invasive option that would allow us to reach the goal.

The state must consider: Is there really a need that clearly outweighs the loss of privacy? Is the proposed measure likely to be effective in achieving the intended purpose? Is the intrusion on privacy proportional to the benefit to be gained? Is there some other less privacy-invasive way to achieve the same goal?

Unfortunately, recent federal initiatives are not always meeting this privacy test.

Technological advancements continue with no sign that governments recognize that amassing and analyzing mountains of personal data – virtually all of it from perfectly ordinary people – may not be the most effective way to protect us.

The threats to privacy have grown dramatically since the Office of the Privacy Commissioner opened its doors – with ever-growing databases, network computing, consumer profiling, and national security concerns. The list of issues has been daunting.

I can only imagine the challenges that a Privacy Commissioner will face a mere 15 years into the future with ubiquitous computing, handheld devices, nanotechnologies and more powerful surveillance techniques.

Despite challenges, our efforts to protect privacy in the public sector are not as effective as they could be given that the privacy law governing federal government programs is desperately outdated.

I can only imagine the challenges that a Privacy Commissioner will face a mere 15 years into the future with ubiquitous computing, handheld devices, nanotechnologies and more powerful surveillance techniques.

Privacy Act Reform

The *Privacy Act* needs to be overhauled.

Our hopes for better privacy protection for Canadians were revived in the spring of 2008, when the House of Commons Standing Committee on Access to Information, Privacy and Ethics announced a review of the *Privacy Act*.

Following this, our strategy was to provide the Committee with proposals that have a realistic chance of being adopted relatively soon. We put forward ten “quick fixes” – simple, straightforward suggestions for improving the legislation. Experts from across Canada, including members of our External Advisory Committee, testified in support of the needed reform.

The changes would go some way to improving privacy protections, but in no way eliminate the need for a highly detailed review and complete overhaul.

We look forward to seeing the Committee’s recommendations. Hopefully there will be some good news to report on legislative reforms in our next annual report.

Privacy Red Flags

The importance of strong protections for personal information held by governments – and the potential risk to citizens if such safeguards are not in place – was vividly demonstrated with a huge data breach in the United Kingdom in late 2007.

An administrative error – sending two unencrypted computer disks through an internal government mail system – compromised the personal information of 25 million people.

Strong privacy legislation can help prevent these sorts of simple but catastrophic mistakes, which leave people at serious risk for identity theft or other harms.

In this annual report, we focus on similarly dramatic shortcomings in how some federal institutions here in Canada are handling the personal information of the citizens they were established to serve.

Audits conducted by our Office uncovered serious problems with the privacy practices of three organizations that hold a great deal of highly sensitive personal information – the

Strong privacy legislation can help prevent these sorts of simple but catastrophic mistakes, which leave people at serious risk for identity theft or other harms.

Royal Canadian Mounted Police (RCMP), Passport Canada, and the Department of Foreign Affairs and International Trade (DFAIT).

RCMP Audit

The privacy issues we discovered while conducting an audit of the RCMP's exempt data banks – designed to prevent public access to the most sensitive national security and criminal intelligence files – were significant enough to prompt us to use our powers to table a special report to Parliament for the first time in the history of my Office.

The audit found that tens of thousands of files sheltered in RCMP exempt data banks should not have been there – raising questions about government transparency and accountability. Canadians should be able to see their personal information unless the disclosure could threaten national security, international affairs or lawful investigations.

The repercussions of such poor information management are potentially grave. People named in an exempt bank file could face serious harms.

Passport Audit

With this annual report, we are releasing the findings of an audit which identified serious flaws in privacy practices and procedures related to Canada's passport operations.

The audit uncovered a worrying series of problems in the way in which personal information is handled by Passport Canada and DFAIT. These problems may put at risk the privacy of Canadians applying for passports.

Training for Public Servants

One of the issues identified in our passport audit was the fact that some of the employees handling applications did not have a clear understanding of their obligation to protect privacy.

Training is essential to ensure all public servants understand their important responsibilities under both the *Privacy Act* and related Treasury Board Secretariat guidelines. Privacy training must be a requirement for public servants who handle significant amounts of personal information.

International Efforts

Our Office is also – by necessity – looking beyond Canada's borders to develop privacy solutions for Canadians.

Transborder data flows and the Internet have transformed privacy into a global issue. Given the speed at which our personal data zips around the globe, assuring Canadians' privacy requires strong international approaches to data protection.

Given the speed at which our personal data zips around the globe, assuring Canadians' privacy requires strong international approaches to data protection.

Privacy protection can no longer be done on a country by country basis. The only way to succeed is by working collectively on privacy and security issues.

Canada is well-positioned to contribute to this effort. Over the years, we've developed a flexible, collaborative approach to data protection in the global context. Traditional close ties to the United States and membership in both the Asia Pacific Economic Cooperation (APEC) and the Organisation for Economic Cooperation and Development (OECD) place Canada in an excellent strategic position to help facilitate cooperation between countries.

I've been honoured to be able to work with the OECD Working Party on Information Security and Privacy. This group's work is key to ensuring that global flows of information are adequately protected. The OECD Recommendation on Cross-border Privacy Co-operation adopted last year was a positive step, but we still have a ways to go.

We have also participated in the work of APEC, which is now implementing the APEC Privacy Framework.

In September, we hosted privacy advocates and experts from around the world at the 29th International Conference of Data Protection and Privacy Commissioners in Montreal, following a 2002 commitment. This conference was an important opportunity to discuss global privacy concerns and solutions. Commissioners resolved to increase cooperation and to help develop universally accepted international privacy standards in the area of information technology.

We will continue our work to encourage the development of global standards which will benefit people around the world.

Farewell to an Assistant Commissioner

Finally, on a more personal note, my Office is bidding *au revoir* to Raymond D'Aoust, Assistant Privacy Commissioner responsible for the *Privacy Act*.

Raymond arrived at the OPC at a very challenging time in the Office's history. A Commissioner and a handful of senior officials had just resigned amid a very public scandal.

Raymond brought the ideal personal attributes to help rebuild morale and resolve an organizational crisis – kindness, sensitivity and a passion for people. He encouraged a balanced approach to work and life – even introducing lunchtime yoga in the office boardroom.

A long career of committed public service provided Raymond with extensive experience in areas such as program evaluation, review, public consultation, strategic planning, business planning and quality management. He used all of this knowledge to make a major contribution to institutional renewal at the OPC.

Gifted with remarkable analytical skills, Raymond was consistently brilliant at identifying all the components of a given situation so he could assess it fairly and properly. A man of principle and a consummate professional, his tireless efforts and effective, firm diplomacy were instrumental to his many successes.

Raymond also brought with him a deep commitment to protecting privacy rights. His efforts have been driven by a strong notion of what the work of this Office means for individual Canadians. He was front and centre on a number of key files, including the protection of DNA, electronic health records, enhanced driver's licences and the no-fly list – to name but a few. I must also congratulate him for his stalwart endeavours to push *Privacy Act* reforms forward. He successfully conducted a number of governmental policy studies and helped found the Association of Francophone Data Protection Authorities.

The Office of the Privacy Commissioner has greatly benefited from his work and we are pleased that he will continue to work with us as Special Advisor to the Commissioners until his retirement.

Un très grand merci Raymond.

A Strong Team

I would also like to thank the rest of the wonderful team in my Office for their dedicated service over 2007-2008. As this annual report illustrates, the issues we work on each day are varied, complex and challenging. We've been lucky enough to attract an exceptionally talented new generation of privacy protection experts to our ranks over the past year.

I offer a special word of thanks to everyone working so hard on our initiatives related to *Privacy Act* reform, international data protection and investigation re-engineering – all of which are critical to ensuring our Office will be a strong, effective guardian of Canadians' privacy rights well into the future.

Jennifer Stoddart
Privacy Commissioner of Canada

KEY ACCOMPLISHMENTS IN 2007-2008

Our Office serves three key client groups – Parliament, federal government departments and agencies, and individual Canadians – under the *Privacy Act*.

Some of our key accomplishments in 2007-2008 include:

Proactively Supporting Parliament

- Tabled the Privacy Commissioner's first special report to Parliament, which outlined the findings of an audit of the RCMP's exempt data banks
- Prepared a submission and appeared before the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182
- Appeared six times before parliamentary committees on such issues as identity theft and the *Canada Elections Act*
- Worked with the Standing Committee on Access to Information, Privacy and Ethics on the statutory review of PIPEDA; responded to Industry Canada's consultation on PIPEDA review
- Joined provincial and territorial privacy oversight officials in passing joint resolutions on the privacy risks associated with enhanced driver's licences, as well as the need for comprehensive changes to the no-fly list program

Serving Canadians

- Responded to 4,258 *Privacy Act*-related inquiries and 2,367 general inquiries
- Investigated hundreds of privacy complaints in the public and private sectors
- Created a blog to help stimulate a discussion with Canadians on privacy issues

- Began work on a social marketing campaign aimed at encouraging awareness and prompting action on children's privacy online
- Participated in court cases in order to help develop privacy-conscious jurisprudence in Canada

Supporting Federal Government Institutions

- Reviewed government policies and initiatives as they relate to privacy legislation and provided input to federal institutions, as well as Parliamentarians
- Reviewed 93 Privacy Impact Assessments

International Highlights

- Hosted the 29th International Conference of Data Protection and Privacy Commissioners, honouring a 2002 commitment
- Joined other international data protection authorities in passing resolutions on the need for global standards for safeguarding passenger data; greater international cooperation on privacy issues; and active involvement in the development of universally accepted international privacy standards in the area of information technology
- Chaired an OECD group working to enhance cooperation between data protection authorities and other privacy rights enforcement agencies around the world; the OECD adopted a recommendation on cross-border cooperation based on the volunteer group's work
- Contributed to an APEC data privacy group's efforts to implement a new privacy framework for APEC members
- Worked with the Standards Council of Canada on the development of international privacy standards
- Joined the International Standards Organization (ISO) and became a member of an important ISO Working Group tasked with developing and maintaining standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data
- Participated in the International Working Group on Data Protection in Telecommunications, which has recently focused on Internet privacy

- Played a lead role in the creation of an international association of data protection authorities and other enforcement agencies from francophone states
- Became a member of the Asia Pacific Privacy Authorities Forum

Encouraging Research and Debate

- Commissioned 22 research projects related to emerging privacy issues
- Issued a consultation paper seeking feedback on the implications of using RFID technology in the workplace
- Published a discussion paper on the role of identity in society and the privacy issues related to identity

PRIVACY BY THE NUMBERS IN 2007-2008

Average number of <i>Privacy Act</i> inquiries per month:	354
Average number of new <i>Privacy Act</i> complaints received per month:	63
Average number of investigations closed per month:	73
Total investigations closed during the year:	880
Privacy Impact Assessments reviewed:	78
Privacy Impact Assessments closed:	93
Parliamentary appearances:	6
Bills/acts reviewed for privacy implications:	19
Research papers issued:	16
Public events organized:	7
Formal visits by external privacy stakeholders:	39
Research activities commissioned:	22
Speeches and presentations delivered:	86
Media requests:	417
Interviews provided:	268
News releases issued:	37
Average hits to our website per month:	128,091
Average hits to our blog per month (September 2007 to March 2008):	17,345
Litigation decisions under <i>Privacy Act</i> :	1

CANADA



PASSPORT
PASSEPORT

PASSPORT CANADA AUDIT: SIGNIFICANT RISK FOR PRIVACY

Lack of adequate safeguards leaves the personal information of passport applicants vulnerable to misuse

Privacy and security problems in Canada's passport operations add up to a significant risk for Canadians applying for passports, an OPC audit has found.

The audit at Passport Canada and the Department of Foreign Affairs and International Trade (DFAIT) unfortunately found weaknesses in every step of the application process; the way in which personal information is collected and stored; how it can be accessed; and how it is ultimately disposed.

For example, passport applications and supporting documents were kept in clear plastic bags on open shelves; documents containing personal information were sometimes tossed into regular garbage and recycling bins without being shredded – and some documents that had been shredded by a private contractor could easily be put back together. Meanwhile, computer systems allowed too many employees to access certain passport files and controls, such as audit logs and encryption, were missing.

These privacy and security shortfalls are particularly worrying given the high sensitivity of the personal information involved in processing passport applications. There is a risk that this information could be used for nefarious purposes if it wound up in the wrong hands.

We are pleased that Passport Canada and DFAIT have indicated they will take action on our recommendations.

These privacy and security shortfalls are particularly worrying given the high sensitivity of the personal information involved in processing passport applications.

Background

Passport Canada processed more than 3.6 million passport applications in 2006-2007. It currently has more than 30 million passport records under its control. The information people provide on their application forms, supporting documentation, as well as passports include highly sensitive personal information.

Passport Canada is an agency of DFAIT, which has a mandate to issue passports. It also provides guidance to DFAIT missions issuing passports abroad.

Missions issued approximately 136,000 passports in the 2006-2007 fiscal year. While that represents only 3.5 per cent of the total number issued, DFAIT has acknowledged that the delivery of passport services abroad is “exposed to a high degree of inherent risk.”

There is a risk of consequences – identity theft, for example – to individual passport holders if their personal information goes missing or is stolen. It’s clear that stronger safeguards are required to protect this data.

Unfortunately, while the passport agency has adopted some good privacy and security features, the audit identified shortcomings. There are a number of opportunities to strengthen the privacy management framework and practices for the passport program.

Privacy Management Framework

Passport Canada does not have a Chief Privacy Officer. In fact, DFAIT has not delegated full authority to Passport Canada for privacy matters. As a result, key privacy responsibilities for the passport program are dispersed and, in our opinion, have not been given sufficient attention.

While the appointment of a Chief Privacy Officer is not a legislated requirement, it is increasingly becoming a practice among federal departments and agencies with significant personal information holdings.

The appointment of a Chief Privacy Officer helps ensure that privacy issues have a champion at the corporate decision-making table. It also ensures accountability for an organization’s privacy management practices.

Collection Issues

Our Office's list of other concerns begins with the passport application itself. Passport Canada concentrates a large amount of sensitive personal information on one application form. Credit card information is collected along with other identifying information, such as names, addresses, phone numbers, birthdates and sometimes Social Insurance Numbers.

Financial information and other personal information – particularly a Social Insurance Number – are key information ingredients sought by identity thieves.

Because an applicant's credit card information is combined with other application form information (both physically and electronically), virtually any employee involved in the passport process can access credit card numbers – even if they don't need this information to process the application.

Too Much Access

Too many DFAIT employees are able to see completed passport documents and the personal information they contain.

Access to personal information on passport applications is not adequately controlled to ensure that only employees who require this information can see it.

For example, consular officials at missions around the world – including locally hired staff – had computer access to passport files processed by any other mission abroad even though the need to access this information was infrequent and the information could be provided by other means on a need to know basis. As a further example, mission staff in one city can access completed passport records from other cities – and vice versa.

Our audit found a case where a former mission employee still had access to the passport management system even though she had left that employment six months earlier. One employee responsible for protocol and official visits had full access rights to the system – though it had nothing to do with his job. Other employees were included on the access list, although they no longer had access to passport records.

Passport Canada has been raising the security level it requires for employees handling passports to the "Secret" level. However, many consular employees, including most locally hired staff, still only have a basic "reliability" security level. In many countries around the world, difficulties in obtaining criminal and intelligence records pose a challenge for raising the security level of locally hired, non-Canadian staff.

DFAIT could mitigate the inherent risk associated with locally hired staff by using better access controls and also keeping track of who is accessing passport files.

We were surprised to find that IT systems for completed passport application files at both Passport Canada and DFAIT lacked a computer safeguard to track who had viewed these records.

The lack of such an audit trail flags a privacy risk in Canada's passport system that – if left unchecked – could lead to undetected security risks and data breaches.

The lack of such an audit trail flags a privacy risk in Canada's passport system that – if left unchecked – could lead to undetected security risks and data breaches.

Security Shortfalls

In some passport offices and missions abroad, passport records and supporting documents were stored in clear plastic bags and left on open shelves on their premises.

Use of portable memory devices, and the lack of encryption for stored personal information, and the transmission of e-mails with passport information outside DFAIT and Passport Canada, all pose a further risk to the protection of personal information.

Neither Passport Canada nor DFAIT has an organization-wide policy restricting employees' use of portable memory devices such as memory sticks and cell phones at work. Such devices are small, easy to use and hold large quantities of data. Anyone with access to passport information systems could photograph or download and copy personal information onto a portable device without being detected.

While our audit was not designed to detect privacy breaches, and none came to our attention during the audit (other than a breach of the Passport On-Line system), it is clear that a great deal of trust is placed in the employees who process passport applications, including locally employed staff. While we recognize the need for trust is inherent in the process, enhanced controls support trust and mitigate risk.

We also found that Passport Canada archives electronic passport records for up to 100 years – even though the reasons for keeping this personal information for such a long period of time are unclear.

The risk that this personal information will be compromised is heightened by the fact that personal information stored on both Passport Canada's main database and DFAIT's passport system is not encrypted. Another information technology concern is that e-mails containing personal information sent outside of secure internal networks may not be protected by encryption and are, therefore, vulnerable to interception and improper use by hackers. Many employees we interviewed were unaware that such e-mails may not be protected.

Our Office also has a number of concerns about the way in which Passport Canada is disposing paper and electronic passport records.

A number of Passport Canada offices and Canadian missions abroad disposed of passport administration forms containing personal information, such as names and dates of birth, in ordinary garbage and recycling bins.

At one private-sector shredding facility under contract with Service Canada, we found that – even after the documents had apparently been shredded – entire passport photos remained intact and documents could be pieced together with little effort.

Finally, the design of consular areas in some missions does not offer adequate privacy for clients. Applicants' sensitive conversations with consular officials can be overheard by other people in public waiting areas.

Online Risks

While our audit was underway, the OPC learned through the media about a breach of Passport Canada's online passport system. An Ontario man using the system had discovered he could access other applicants' sensitive passport information by randomly changing one number in the Uniform Resource Locator, or URL, which appears at the top of each page on every Internet site.

Passport Canada shut down the system and corrected the programming problem.

The agency told us that the incident was the only breach of this type it was aware of. Given that the man who had seen other people's personal information had immediately reported the breach to Passport Canada, the risk to Canadian's passport information was considered minimal by the agency. Passport Canada is investigating further and we are awaiting a full report.

Passport Canada has plans to replace the online system within a year with a new method to encrypt and protect personal data.

Recommendations and Next Steps

Our Office provided Passport Canada and Foreign Affairs with 15 recommendations to strengthen the privacy management framework for passport operations.

These include:

- Hiring a Chief Privacy Officer at Passport Canada
- Providing ongoing privacy and security training programs to staff
- Introducing better controls on access to passport information
- Reassessing the current 100-year retention period for passport information
- Providing essential safeguards, including: more restricted access to areas where passports are processed; privacy for clients discussing passport applications; re-evaluating adequacy of security screening for employees; policies on portable memory and recording devices, such as cell phones; and expanded use of encryption

Further to our audit report, both Passport Canada and DFAIT have agreed with most of our recommendations.

We will follow up with Passport Canada and DFAIT on our recommendations with a post-audit.

We would like to thank Passport Canada and DFAIT employees for their professionalism, cooperation and responsiveness during our audit.

The full audit report, including management responses, is available on the OPC website.



ADMINISTRATIVE AND QUASI-JUDICIAL BODIES: *BALANCING OPENNESS AND PRIVACY IN THE INTERNET AGE*

Complaints to the OPC highlight concerns about federal administrative and quasi-judicial tribunals posting highly sensitive personal information to the web

Highly personal information about Canadians fighting for government benefits and taking part in other federal administrative and quasi-judicial proceedings is being posted to the Internet – exposing those people to enormous privacy risks.

In 2007-2008, the OPC investigated 23 complaints regarding the disclosure of personal information on the Internet by seven bodies created by Parliament to adjudicate disputes. (We received three more similar complaints in May 2008.)

These administrative and quasi-judicial bodies consider issues such as the denial of pension and employment insurance benefits; compliance with employment and other professional standards; allegations of regulatory violations; and irregularities in federal public service hiring processes.

The adjudication process often involves very intimate details related to people's lives, including their financial status, health, job performance and personal history.

Few would question the fundamental importance of transparency in tribunal proceedings.

But is it in the public interest to make considerable amounts of an individual's sensitive personal information indiscriminately available to anyone with an Internet connection?

Why should a law-abiding citizen fighting for a government benefit be forced to expose the intimate details of her personal life to public scrutiny?

Why should a law-abiding citizen fighting for a government benefit be forced to expose the intimate details of her personal life to public scrutiny?

The Human Impact

The decisions of administrative and quasi-judicial decision-makers are routinely packed with personal details that not many people would be comfortable sharing widely: salaries, physical and mental health problems as well as detailed descriptions of disputes with bosses and alleged wrongdoing in the workplace.

In addition to the types of personal information legitimately needed in these bodies' reasons for decision, seemingly irrelevant information is often included – the names of participants' children; home addresses; people's place and date of birth; and descriptions of criminal convictions for which a pardon has been granted, for example.

Many complainants told us they were distressed to discover – typically with no prior notice – that this type of information about them was available on the Internet for neighbours, colleagues and prospective employees to peruse.

The following are some of the comments we heard:

"By posting my name, I feel violated in my privacy and this could adversely affect my prospects for jobs, business and my image in the community. I have never given consent."

"Anybody, anywhere in the whole world, who types my name comes immediately to this personal information.... this situation leaves me open to criticism and mockery."

"I'm at a loss to understand why this would have been done, except to think that this is further punitive measures taken against me."

The potential for embarrassment, humiliation and public ridicule is significant. A long-ago legal transgression or temporary lapse in judgment could continue to haunt an individual for many, many years into the future.

Individuals whose personal information, particularly financial information, is disclosed on the Internet may be at greater risk of identity theft. They also face a risk of discrimination, harassment and stalking. The information could also be used by data brokers that compile profiles of individuals.

"Anybody, anywhere in the whole world, who types my name comes immediately to this personal information.... this situation leaves me open to criticism and mockery."

A list of the bodies whose practice of posting personal information online have resulted in complaints investigated by the OPC in 2007-2008:

Canada Appeals Office on Occupational Health and Safety

The Canada Appeals Office on Occupational Health and Safety (CAO), now known as the Occupational Health and Safety Tribunal Canada, is a quasi-judicial administrative tribunal that determines appeals of decisions and directions issued by health and safety officers. It operates under the auspices of Human Resources Development Canada. Decisions rendered by this tribunal may include an individual's name, coupled with that person's personal opinions or views and place of employment.

Military Police Complaints Commission

The Military Police Complaints Commission is an independent federal body that oversees and reviews complaints about the conduct of Military Police members. The Commission is empowered to: review the Provost Marshal's handling of complaints concerning the conduct of Military Police; deal with complaints alleging interference in military police investigations; and conduct its own investigations or hearings related to complaints when the Commission believes that doing so is in the public interest.

All of the Military Police Complaints Commission decisions are vetted by the Commission with a view to the standards expressed in the *Privacy Act*. Most decisions rendered by the Military Police Complaints Commission are published on the Internet in summary and depersonalized form. Where decisions are not depersonalized, they may contain extensive personal information about military police members.

Pension Appeals Board

The Pensions Appeal Board is responsible for hearing appeals flowing from decisions of the Canada Pension Plan Review Tribunals. A hearing before the board may be initiated by an individual seeking Canada Pension Plan (CPP) benefits or by the Minister of Social Development. The board has the authority to determine, among other things, whether benefits under the CPP are payable to an individual.

Board decisions reveal a considerable amount of sensitive personal information about individuals seeking benefits, including dates of birth, detailed family, education and employment histories, extensive personal health information and personal financial data.

Public Service Commission

The Public Service Commission is a quasi-judicial tribunal that may conduct investigations and audits on any matter within its jurisdiction, including safeguarding the integrity of appointments and in overseeing the political impartiality of the federal public service. Its decisions may include information relating to individuals' education or medical or employment history.

Public Service Staff Relations Board

The board, which has been replaced by the Public Service Labour Relations Board, was a federal tribunal responsible for administering the collective bargaining and grievance adjudication systems in the federal public service.

Decisions may include descriptions of individuals' conduct and issues at work as well as disciplinary sanctions they've faced.

RCMP Adjudication Board

An RCMP Adjudication Board conducts formal disciplinary hearings respecting RCMP members' compliance with the Code of Conduct adopted under the *Royal Canadian Mounted Police Act*. Decisions include information about alleged misconduct, and, in some cases, other personal information such as an officer's marital situation and medical information. Adjudication Board decisions, which include the names of individuals, are published on the RCMP intranet, although the Board has advised that it intends to post its decisions on the Internet.

Umpire Benefits Decisions (Service Canada)

The *Employment Insurance Act* permits claimants and other interested parties to appeal to an umpire certain decisions rendered under that Act. An umpire is empowered to decide any question of fact or law that is necessary for the disposition of an appeal.

Decisions by an umpire tend to reveal detailed information about the employment history of claimants. A typical decision might also reveal information about a claimant's place of residence, marital status and sources of income.

Access to Justice

Another concern we have is that access to justice could suffer if tribunals, boards and other administrative decision makers continue to post decisions on the Internet.

The risk of having one's personal details made public may make people increasingly reticent to assert their rights in administrative and quasi-judicial proceedings. People trying to obtain benefits required to provide food and shelter for themselves and their families may feel that participation in tribunal proceedings is essentially mandatory – and that they have no option other than to give up their right to privacy.

In some cases, however, individuals have declined to exercise their legal right to appeal administrative decisions that significantly impacted them because of the loss of privacy this would entail.

“Open Court” Principle

The widespread practice of posting reasons for decisions on the Internet appears to be based on the assumption by decision makers that the rules – or lack of rules – which apply to judicial proceedings apply equally to administrative and quasi-judicial proceedings.

Many of the institutions investigated argued that the “open court” principle required the online publication of decisions.

The open court principle is an important part of our legal system and exists to ensure the effectiveness of the evidentiary process, encourage fair and transparent decision-making, promote the integrity of the justice system and inform the public about its operation. Opening decision-making processes up to public scrutiny assists to further these goals.

However, there is an important distinction between the courts and the institutions we investigated. The *Privacy Act*, which does not apply to the courts, applies to many administrative tribunals and quasi-judicial bodies and imposes specific rules on them regarding the disclosure of personal information. Through the *Privacy Act*, Parliament may be said to have set express limits on the extent to which the open court principle could authorize publication of decisions of the administrative tribunals subject to its provisions via the Internet.

Striking a Reasonable Balance

Respect for the open court principle can co-exist effectively with government institutions' statutory obligations under the *Privacy Act* through reasonable efforts to depersonalize any decisions posted online by replacing names with random initials.

It is beyond debate that the public requires access to the information necessary to maintain confidence in the integrity of a tribunal's proceedings, to enhance the evidentiary process, to promote accountability and to further public education. Yet in most cases, these important goals may be accomplished without disclosing the name of an individual appearing before a tribunal.

The identity of individuals appearing before tribunals is not obviously relevant to the merits of any given tribunal decision. As the open court principle is intended to subject *government institutions* to public scrutiny, and not the lives of the *individuals* who appear before them, the OPC has taken the position that the public interest in accessing information about tribunals' proceedings does not obviously or necessarily extend to accessing identifying information about individual participants.

Furthering the values that the open court principle promotes will not be hindered if, consistent with government institutions' obligations under the *Privacy Act*, only de-personalized decisions that do not reveal the identities of participants are made available to the public. It is, of course, also open to tribunals to redact all personal information that would otherwise be found in reasons for decision made available to the public. However, simple suppression of direct and obvious identifiers such as names is likely to represent the most efficient and effective means of complying with the *Privacy Act*. This method of protecting privacy poses no significant threat to tribunals' independence and ensures that the facts and issues in individual cases may be fully and transparently debated in an open and accessible manner.

Where there is a genuine and compelling public interest in disclosure of identifying information that clearly outweighs the resulting invasion of privacy, institutions have the legal authority to exercise their discretion to disclose personal information in identifiable form in their decisions. For example, where the public has a compelling interest in knowing the identity of an individual who has been found guilty in disciplinary proceedings, or of someone who poses a potential danger to the public, a tribunal may exercise its discretion to disclose personal information, including that individual's name, to the public.

Likewise, where Parliament or a body empowered to make regulations has drafted a law or regulation that authorizes the disclosure of personal information, the *Privacy Act* permits disclosure of personal information in accordance with such a provision. In this way, the Act recognizes the right of lawmakers to craft disclosure regimes that are responsive to particular tribunals' mandates and the associated demands of the open court principle.

There is, thus, no intractable conflict between the rights and interests protected by the open court principle and compliance with the *Privacy Act*.

It is also noteworthy that courts, too, are increasingly recognizing the need to limit the disclosure of personal information in judgments. The Canadian Judicial Council has published a Recommended Protocol for the use of personal information in judgements. This protocol recognizes it can be appropriate for judges to omit some personal information from a judgment in the interests of protecting privacy. Where appropriate, these guidelines encourage the judiciary to omit from judgments personal data identifiers, highly specific personal information and extraneous personal information with little or no relevance to the conclusions reached.

Privacy Act Limits

During our investigation, we found there is a significant lack of consensus among administrative and quasi-judicial decision-makers on the limits that the *Privacy Act* places on the Internet disclosure of personal information in their decisions.

The decisions of most, if not all, institutions subject to the *Privacy Act* contain personal information to which the protections of the legislation apply.

The *Privacy Act* says that personal information under the control of a government institution may be disclosed for the purpose for which it was obtained or compiled, or for a use consistent with that purpose.

The OPC concluded that the blanket electronic disclosure of these bodies' reasons for decision on the intranet or Internet is not the purpose for which the information was obtained. Rather, tribunals collect personal information for the purpose of making a decision on the facts of each specific case before them.

Moreover, disclosing administrative or quasi-judicial decisions with identifiable personal information on the Internet as a matter of course was not found to be reasonably necessary for the accomplishment of the investigated institutions' mandates. It was not a disclosure for a use that was consistent with the purpose for which the personal information was obtained — particularly when the uses to which sensitive personal information would be put could not be identified in advance or controlled in any way.

Under the *Privacy Act*, limits on the disclosure of personal information do not

...disclosing administrative or quasi-judicial decisions with identifiable personal information on the Internet as a matter of course was not found to be reasonably necessary for the accomplishment of the investigated institutions' mandates.

apply to publicly available information. Some of the institutions investigated argued that the publicly accessible nature of administrative and quasi-judicial proceedings rendered the personal information discussed during those proceedings publicly available for the purposes of the Act.

However, none of those institutions presented any evidence to indicate there was any record, in any form, of the personal information disclosed during the course of proceedings that is available in the public domain. Our Office found that disclosure of personal information during a proceeding did not in itself render that information available in the public domain.

The *Privacy Act* also allows for disclosure of personal information in accordance with any Act of Parliament or regulation authorizing such a disclosure.

Some institutions argued that the disclosure of personal information was permissible due to the fact that relevant legislation or regulations did not prohibit or address disclosure. We rejected this argument. There must be some specific indication in an Act or regulation that Parliament intended to permit disclosures of personal information outside of the quasi-constitutional regime created by the *Privacy Act*. Legislative silence on the issue does not constitute a legal authority to disclose personal information.

Recommendations

In the well-founded complaints we investigated, our Office made a number of recommendations to government institutions:

- Reasonably depersonalize future decisions that will be posted on the Internet through the use of randomly assigned initials in place of individuals' names; or post only a summary of the decision with no identifying personal information.
- Observe suggested guidelines respecting the exercise of discretion to disclose personal information in any case where an institution proposes to disclose personal information in decisions in electronic form on the Internet.
- Remove decisions that form the basis of the complaints to the OPC from the Internet on a priority basis until they can be reasonably depersonalized through the use of randomly assigned initials and re-posted in compliance with the *Privacy Act*.
- Restrict the indexing by name of past decisions by global search engines through the use of an appropriate "web robot exclusion protocol;" or remove from or reasonably depersonalize all past decisions on the Internet through the use of randomly assigned initials, within a reasonable amount of time.

Response to OPC Concerns

Even after being advised of privacy issues, most government institutions were reticent to change their policies and practices.

Notwithstanding the growing number and severity of privacy threats to individuals whose personal information is posted indiscriminately on the Internet, some government institutions told us they plan to continue posting sensitive personal information as they always have.

Others took important but incomplete steps towards improved compliance with the *Privacy Act*. As a result of our investigations, some institutions have implemented technical measures to prevent the names of individuals who participate in their decision-making processes from creating “search hits” when typed into major search engines. Others have agreed to use initials in place of individuals’ names.

Notably, Service Canada and Human Resources Development Canada agreed to fully implement our recommendations.

The OPC has relayed the results of its investigation to the complainants. In cases where these results were disappointing, the OPC remains committed to working with the bodies involved with a view to improving privacy protections for those who participate in administrative and quasi-judicial processes.

The varying degrees of responsiveness to the OPC’s recommendations means that, even among those institutions investigated, there remains inconsistent privacy protection for Canadians who participate in these institutions’ administrative and/or quasi-judicial proceedings.

It is also worth noting that many other administrative and quasi-judicial bodies post online reasons for decisions that link identifiable individuals with a great deal of sensitive personal information, but the OPC has not received complaints about them.

Next Steps

Under the *Privacy Act*, this is not a matter that we are empowered to bring before the courts for further guidance.

However, our Office is committed to continuing to work with the government institutions which have been reluctant to implement all of the recommendations. We hope that by maintaining a constructive dialogue, we will be able to persuade these organizations to take the steps necessary to protect Canadians’ privacy.

We also see a need for a new government-wide policy on this privacy issue. Given the complexity of the issues involved, recommendations flowing from our investigation of a small number of institutions are not the best instruments around which to build government-wide compliance with the *Privacy Act*. A comprehensive policy document based on consultations with a wider range of government institutions is required.

We hope that by maintaining a constructive dialogue, we will be able to persuade these organizations to take the steps necessary to protect Canadians' privacy.

We have already conveyed to the Treasury Board Secretariat our view that centralized policy guidance is required. This guidance will ensure consistency in the privacy protection available to Canadians who participate in administrative and quasi-judicial proceedings.

Many institutions we investigated agreed with our view that centralized policy guidance is required and would welcome the same. They were willing to participate in consultations with Treasury Board to develop policy guidance and comply with this guidance when it took effect.

Treasury Board has advised our Office that its officials continue to work on developing guidance for federal institutions subject to the *Privacy Act* with respect to the posting of personal information on government websites. Treasury Board has also indicated that it will consult with our Office on any draft guidance that is developed.

Electronically publishing personal information contained in the administrative and quasi-judicial decisions of government institutions is risky privacy business. We look forward to working with Treasury Board on this important issue to ensure Canadians' privacy will be better protected by strong policy guidance in the future.

The trend to put more and more federal government information online raises important questions about how to balance the public interest and individual privacy rights.

While the use of the Internet to promote transparency and accountability in the federal government – posting contracts and travel expenses, for example – is a welcome development, it is clear there must be limits when it comes to the disclosure of personal information.



PRIVACY TRAINING IN THE FEDERAL PUBLIC SERVICE:

THE NEED FOR A COMPREHENSIVE APPROACH

Providing all employees who handle personal information with privacy training is one of the key ways in which governments can prevent data breaches

In late 2007, a relatively simple mistake by a British civil servant led to one of the biggest data breaches in history.

The incident compromised the personal information of 25 million people receiving a child benefit – and stands as a cautionary tale for governments around the world about the need to take data protection, including employee privacy training, extremely seriously.

An official in the U.K.'s Revenue and Customs Office had placed two computer disks containing details about families registered in a child benefit database into an envelope to be couriered to another government department.

The CDs did not arrive at their destination and have yet to be recovered.

The breach, which exposed families across Britain to the risk of identity theft, resulted in the resignation of the chairman of the Revenue and Customs Office and led to a major police investigation.

After its investigation, the British Independent Police Complaints Commission concluded that individual staff members were not to blame. Instead, it said “woefully inadequate” data handling practices and procedures, including a lack of training for staff, led to the breach.

“There was: a complete lack of any meaningful systems; a lack of understanding of the importance of data handling; and a ‘muddle through’ ethos,” the Commission said. “Staff found themselves working on a day-to-day basis without adequate support, training or guidance about how to handle sensitive personal data appropriately.”

Following the breach, the British government introduced mandatory annual training for all civil servants who deal with personal data.

Here in Canada, the OPC has for some time been urging the federal government to provide better training for public servants on the fundamental principles of personal information management. This privacy training should be mandatory for all managers and all public servants who handle personal information.

Privacy training should be mandatory for all managers and all public servants who handle personal information.

Unless adequate learning programs are put in place, a regrettable incident could lead to a breach of personal data held by a federal department or agency. Such a breach could affect thousands – if not millions – of Canadians.

Over the last few years, we have seen a number of significant breaches of personal information occurring all over the world, in both private and public sector organizations.

These breaches often take the form of the inadvertent or negligent loss of personal data by employees or the theft of equipment containing such data. In many of these cases, the breaches could have been avoided if employees handling the personal information had received training on the fundamental principles of secure and responsible information management.

Audit Concerns

Recent OPC audits underscored the need for comprehensive privacy training for employees who handle personal information in federal government departments and agencies.

In October 2007, our Office published the results of an audit assessing the effectiveness and outcome of Privacy Impact Assessments (PIAs) conducted by federal government departments and agencies for new or redesigned programs and services.

One of the audit's principal conclusions was that more training is needed to ensure that program managers understand their responsibilities under the Treasury Board Policy on Privacy Impact Assessments, and have the privacy knowledge and skills necessary to conduct effective PIAs.

While some government institutions have made a serious effort to apply the policy, the audit found more is required to ensure PIAs are having the desired effect – namely to establish and enshrine privacy protection as a core consideration in government program

and service delivery. The audit also discovered an uneven application of the policy, including a number of performance failures. Our auditors attributed these disappointing results to many causes, including a lack of training.

Another major audit, described in detail in our 2005-2006 annual report, examined the management practices of the Canada Border Services Agency (CBSA) with regards to trans-border data flows and found similar challenges with regards to training needs of key personnel.

Generally, the audit identified significant opportunities for the CBSA to better manage privacy risks and achieve greater accountability, transparency and control over the trans-border flow of personal information.

The audit called for providing regular and ongoing training sessions on the administration of, and compliance with, the *Privacy Act*. It recommended designing and implementing a privacy management framework for the CBSA, a component of which would be the creation of a committee of senior managers mandated with ensuring that privacy guidance and training are provided.

Finally, the audit recommended the development of specific training modules to combat problems with verbal exchanges of personal information between Canadian and U.S. border officials.

An audit of Canada's passport operations, detailed earlier in this report, also highlighted how a lack of adequate training can lead to privacy and security risks.

A Core Curriculum

Some federal government departments and agencies have recognized the need for better privacy training for employees. Statistics Canada and Citizenship and Immigration have introduced training regimes and formal instruction to raise awareness of privacy issues and legislation. The Treasury Board Secretariat has also been providing training for some years to the ATIP community. In addition, the Secretariat provides ongoing advice to individual institutions – both ATIP and program officials – on specific privacy-related issues.

Despite these success stories, on the whole we feel the federal government could be doing much more.

Part of the problem lies in the fact that there is no mandatory core curriculum for educating public servants who process or manage personal information about their basic duties and responsibilities under the *Privacy Act*.

Nor is there a mandatory core curriculum for training these employees on widely recognized privacy fair information principles, which govern the appropriate collection, use, disclosure, and disposal of personal information within government.

The Canada School of Public Service offers two training modules on privacy and access laws. However, these are not mandatory. (The two current courses will be merged into one new course beginning in early 2009.)

Many departments and agencies have designed their own training programs, but in most cases this training is insufficient.

The Public Service Commission of Canada (PSC), for example, runs information sessions to provide advice and training to its managers about the impact of the *Privacy Act* on various programs. The sessions are so popular that the PSC turned some of its managers away in 2007 for lack of resources to provide training. The PSC has since expanded the program in an attempt to meet the demand.

The Department of Foreign Affairs and International Trade has built a permanent policy, process, and training regimen to ensure that all access to information and privacy analysts receive the training they need to do their jobs. However, the department is of the view that there is a pressing need for more widespread training.

Clearly, some departments are willing to meet that need with proactive programs that formalize privacy training. What they need is additional training support to get the job done.

A Comprehensive Approach

The OPC is of the view that a coordinated and comprehensive strategy needs to be developed and implemented by key players in the federal government: the Canada School of Public Service (CSPS); Treasury Board Secretariat (TBS); and ATIP offices in every federal government department and agency.

The Role of the Canada School of Public Service

The Canada School of Public Service's key mandate is to ensure all public service employees have the knowledge and skills they need to develop policy and deliver services for Canadians.

We believe that the School should develop a core, mandatory privacy training curriculum to be used by all government departments and agencies in training employees who handle significant amounts of personal information. The target audience for the core curriculum should be employees up to and including supervisors. Teaching modules and a trainers'

guide should be developed in consultation with the key government institutions in Ottawa that handle significant amounts of personal information.

The School should also develop a distinct mandatory training module for all middle- and senior-level government managers, acquainting them with the fundamentals of privacy and personal information management. This module could be integrated into existing courses for managers, or offered as stand alone courses, as required. (While the School currently offers two training modules on privacy and access laws, these are not mandatory and their target audience consists of functional specialists and supervisors as well as managers.)

Development of the core curriculum, teaching module and trainers' guide should be done in consultation with the Offices of the Privacy Commissioner and the Information Commissioner.

The Role of ATIP Units

We believe that individual ATIP units should play the lead role in dispensing privacy training to employees and supervisors within their respective departments and agencies.

The foundation of the training provided would be the core curriculum and trainers' guide developed by the CSPS, described above. We recognize, however, that training needs may vary from one department or agency to another. Indeed, federal government institutions that handle large amounts of personal data—such as the Canada Revenue Agency or the Canada Border Services Agency—will have different training requirements than a department that handles comparatively little personal information, such as the Department of Finance. That is why we believe that departments and agencies should be free to adapt the core curriculum and trainers' guide to their particular needs and situations.

Treasury Board Secretariat's Role

TBS is responsible for government-wide administration of the *Privacy Act*. The Secretariat coordinates the administration of the Act by preparing and distributing policies and guidelines to help institutions interpret the law and to assist them in their application on high profile issues.

We believe TBS should make mandatory the training we have described above throughout the federal public service. Indeed, TBS needs to continue to play a leadership role in promoting and overseeing privacy training and awareness across the entire federal public service. Its role and importance in ensuring a culture of privacy within the public service cannot be understated.

The Creation of “Privacy Training Champions”

Every department and agency should consider appointing a “privacy training champion” whose mandate would be to oversee and promote privacy training and learning across that institution. This individual should be a member of the senior management team, possibly the organization’s chief privacy officer.

In keeping with the recommendation the OPC made in its audit of the Canada Border Services Agency, every government institution should consider creating a committee of managers mandated with ensuring that requisite guidance and training are provided to programs areas on privacy issues.

Training Content

The key objective of a privacy training program should be to provide public servants with grounding in federal government requirements respecting the protection of personal information holdings, and the knowledge of best practices for managing personal information.

In order to accomplish this, a privacy training program for public servants would need to address certain key themes and subject matters:

- **Knowledge of Statutory and Policy Requirements:** Public servants must understand their duties and responsibilities under the *Privacy Act*, attendant regulations, and other statutory instruments germane to privacy. (Individual departments and agencies may also need to tailor their training programs to take into account special requirements under the legislation they administer, as well as internal policies respecting data management.)
- **Knowledge of What Constitutes Personal Information:** Public servants who manage personal information need a solid grounding in the definition of personal information – recorded information about an identifiable individual – and what this can include.
- **Knowledge of Basic Principles:** Federal public servants need to know what personal information they can collect, use and disclose in the course of their duties. And they need to know how to maintain personal information in a secure manner. Knowledge of the basic principles of privacy – often referred to as “fair information principles” – is essential.
- **Knowledge of Best Practices:** Some techniques, methods and processes are better than others at delivering positive privacy promotion and protection outcomes.

Providing public servants with a strong knowledge of these techniques will help ensure the personal information of Canadians held by government institutions is managed with limited problems or unforeseen complications. Best practices from federal government institutions, as well as those from other jurisdictions – the provinces, foreign governments and the private sector – should be built into the training program.

Conclusion

The federal government needs to address the privacy training and learning needs of its employees head on. And it needs to do so immediately, before a regrettable incident similar to the one in the U.K. occurs.

Public servants who manage the personal information of Canadians are stewards of a public trust that underpins our system of government.

Public servants who manage the personal information of Canadians are stewards of a public trust that underpins our system of government.

Public servants require sound knowledge of the laws, rules, regulations and policies governing privacy and the management of personal information in the federal government. They need a firm understanding of what constitutes personal information; the basic principles of privacy protection and fair information practices; and an appreciation of the best practices for managing personal information.

This specialized knowledge can only be acquired through a comprehensive and coordinated training program for all federal public servants who manage personal information. The Treasury Board Secretariat and the Canada School of Public Service have a leadership role to play in this regard. ATIP units within individual government departments and agencies also have a key role to play, as they are best placed to dispense the knowledge that staff in their institutions require.

The OPC remains ready to help all of these key players with the development of a privacy training curriculum for the federal government.

A comprehensive approach to privacy training and learning is one of the key elements required to safeguard the personal information of Canadians.

UPDATE ON *PRIVACY ACT* REFORM: FIRST STEPS TOWARD LEGISLATIVE OVERHAUL

OPC proposes a series of “quick fixes” to improve Canada’s public sector privacy legislation in the short term

Privacy Commissioners have been calling for reform of the *Privacy Act* for many years now and the increasingly urgent need for modernization of the legislation has become a regular theme of our annual reports.

This year is no different. Our current legislation does not adequately protect the personal information of Canadians held by government departments and agencies.

In 2006, our Office issued a comprehensive report detailing recommended changes to the *Privacy Act*.

Since then, we have consulted with external stakeholders on this issue. For example, we asked the Public Policy Forum to organize two roundtable discussions on reform of the federal privacy regime in June and October 2007. These discussions involved senior government officials who have a stake in privacy promotion and protection.

As we were working on this annual report, we received word from the House of Commons Standing Committee on Access to Information, Privacy and Ethics that its members planned to take a look at the *Privacy Act*.

The committee heard from a number of witnesses. Our Office hopes the committee members will return to this work in the fall of 2008.

Given that there seems to be little appetite in government for a major rewrite of the legislation, the Commissioner proposed a list of 10 “quick fixes” when she appeared before the committee in April 2008. These relatively straightforward changes would address some of the legislation’s shortcomings – basics such as introducing a “necessity test” for the collection of personal information by government departments.

However, the proposals are most emphatically *not* meant to be the definitive statement on *Privacy Act* reform. Our Office sees these 10 recommendations as a first step in modernizing the legislation while we wait for a comprehensive modernization initiative.

Some of the proposed changes would simply incorporate into the law existing federal government policies and practices. Treasury Board Secretariat has done some good work on privacy matters by providing guidance to line departments, for example, on signing information-sharing agreements and the outsourcing of personal data processing. However, amending the legislation would provide clearer guidance in this regard.

Other proposed changes would correspond to provisions that already exist in or are being contemplated for PIPEDA.

Our Office sees these 10 recommendations as a first step in modernizing the legislation while we wait for a comprehensive modernization initiative.

10 *Privacy Act* "Quick Fixes"

- 1 "Necessity test" requiring government institutions to demonstrate need for personal information they collect.
- 2 Broaden grounds for an application for Court review under section 41 of the *Privacy Act*; give Federal Court the power to award damages against offending institutions.
- 3 Requirement to assess privacy impact of programs prior to implementation and to publicly report assessment results.
- 4 Clear public education mandate.
- 5 Greater discretion to report to Canadians on government institutions' privacy management practices.
- 6 Discretion to refuse/discontinue complaints where investigation is not in public interest.
- 7 Eliminate restriction that *Privacy Act* applies only to recorded information.
- 8 Require government institutions to report annually on a broader spectrum of privacy-related activities.
- 9 Require ongoing five-year Parliamentary review of *Privacy Act*.
- 10 Stronger provisions governing disclosure of personal information by Canada to foreign states.

The following is a description of the OPC's proposed "quick fixes":

- 1 Create a legislative "necessity test" which would require government institutions to demonstrate the need for the personal information they collect.

Background

This "necessity test" is already included in Treasury Board policies as well as PIPEDA. It is an internationally recognized privacy principle found in modern privacy legislation around the world. For example, the provinces and territories have adopted a model in their public sector legislation requiring that one of three conditions be met: the collection is expressly authorized by statute; the information is collected for the purpose of law enforcement; or the information relates directly to *and is necessary* for an operating program or activity.

The *Privacy Act* currently states: "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution." This sets a disproportionately low standard for the fundamental rights at the heart of the *Privacy Act*.

What difference would it make?

By building in better controls at the collection point, there is less potential for misusing and disclosing personal information.

- 2 Broaden the grounds for which an application for Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Background

Currently, the Federal Court may only review a refusal by a government institution to grant access to personal information requested by an individual under the *Privacy Act*.

Although the Commissioner can investigate complaints concerning the full array of rights and protections under the legislation and make recommendations, if the response of the institution is not satisfactory, neither the individual nor the Privacy Commissioner may apply to the Federal Court for enforcement and remedy. This means there are no effective remedies for violations of privacy rights, such as the wrongful disclosure of personal information or the inappropriate collection of information.

This is a far lower standard than in the private sector, where PIPEDA provides such remedies for Canadians.

What difference would it make?

Broadening Federal Court review would ensure government institutions respect individuals' rights to have their personal information collected, used and disclosed in accordance with the *Privacy Act*. It would also put the *Privacy Act* on par with PIPEDA.

Every right needs a remedy in order to have meaning.

- 3** Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Background

A 2002 Treasury Board Secretariat policy on Privacy Impact Assessments (PIAs) was designed to assure Canadians that privacy principles would be taken into account during the development and implementation of programs and services that raise privacy issues.

Unfortunately, the way in which institutions are implementing this policy has been uneven. As reported in our 2006-2007 annual report, an OPC audit found that PIAs are not always conducted when they should be and are frequently completed well after program implementation, or not at all.

What difference would it make?

A legal requirement for PIAs would ensure they are done on a consistent and timely basis.

As well, PIAs should be submitted to the OPC for review prior to program implementation – allowing our Office to offer recommendations on how privacy could be better protected.

- 4** Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.

Background

While the OPC's central function under the *Privacy Act* is the investigation and resolution of complaints, the OPC also needs to advance privacy rights by other means – through research, communication and public education. The Commissioner lacks a clear legislative mandate under the *Privacy Act* to educate the public about their privacy rights with respect to information held by federal government institutions.

What difference would it make?

A clear public education authority would allow the OPC to publish public advisories and education material on significant policy and legislative measures with "personal information" components.

PIPEDA contains such a mandate and it is only logical that the *Privacy Act* contain a similar mandate for the public sector.

- 5 Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.

Background

As it now stands, our Office reports to Parliament and Canadians through annual or special reports. There is no specific section in the legislation authorizing the Commissioner to make public interest disclosures.

The OPC has been hampered in its ability to speak with the press, the public, and even Members of Parliament, due to the existing confidentiality constraints in the *Privacy Act*.

Waiting until the end of the reporting year to tell Canadians about privacy issues related to federal institutions means the information has sometimes become moot, stale or largely irrelevant. A clear discretion for public interest disclosures would allow for more timely and relevant public discussions about privacy issues important to Canadians.

What difference would it make?

This discretion would be an important tool for advancing public understanding, providing public assurances, and restoring public confidence where required.

Canadians would have timely information about how the federal government is handling their personal information.

- 6 Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Background

At the moment, valuable resources are still being disproportionately consumed by having to open and investigate all individual complaints on a first-come, first-serve basis. Examples of complaint types where relatively little is gained by investigating include:

- Repetitive issues that have already been clearly decided in past cases (e.g. legitimate collection and use of Social Insurance Numbers.)
- Moot time complaints where the individual has since received the information requested (e.g. where access was already provided, though technically out of

time and at no disadvantage to the individual.)

- Frequent complaints brought forward by the same individual against an institution (e.g. where contentious labour or employment issues constitute the real dispute.)
- Multiple complaints brought by many individuals about the same incident (e.g. a large data breach.)
- Issues that have already been recognized and addressed by a government institution.

Many data protection authorities in Canada and elsewhere face similar challenges in having to treat all complaints received indiscriminately, with no ability to dismiss or discontinue some of them early on where no public interest would be served by investigating or continuing to investigate them.

What difference would it make?

This discretion would allow our Office to focus more investigative resources on privacy complaints which are of broad systemic interest and affect the interests of a significant number of Canadians.

- 7 Amend the *Privacy Act* to align it with the *Personal Information Protection and Electronic Documents Act* by eliminating the restriction that the *Privacy Act* applies to recorded information only.**

Background

Unrecorded information – such as surveillance cameras that are used to monitor people, but do not record images – is beyond the scope of the *Privacy Act*. Personal information contained in deoxyribonucleic acid, known better as DNA, and other biological samples is not explicitly covered.

Under PIPEDA, personal information includes personal information in any form.

What difference would it make?

Expanding the definition of personal information would ensure the *Privacy Act* is responsive to the digital imagery and biometric applications of contemporary law enforcement surveillance and monitoring activities. It would also offer protection for DNA and other biological samples.

- 8 Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act*, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

Background

The *Privacy Act* requires the head of a government institution to submit an annual report to Parliament on the administration of the Act. Our experience in reviewing these reports over the years indicates that, on the whole, they have rarely contained substantive information. Rather, they've tended to be a patchwork of statistics about the number of *Privacy Act* requests received; dispositions taken on completed requests; exemptions invoked or exclusions cited; and completion times.

Treasury Board Secretariat issued comprehensive privacy reporting guidelines for government institutions in 2005, and updated these in early 2008. The *Privacy Act* should be amended to integrate these guidelines into legislation in order to provide them with added weight and authority.

What difference would it make?

A more comprehensive coverage of privacy management issues would provide Parliamentarians with relevant information to evaluate the extent to which government institutions are addressing privacy challenges, and whether new initiatives may pose a threat to the privacy rights of citizens. Individuals would also be better informed on how government departments and agencies are handling their personal information.

- 9 Introduction of a provision requiring an ongoing five-year Parliamentary review of the *Privacy Act*.

Background

The privacy landscape is dynamic and constantly evolving. It is not unreasonable to expect that Parliament should review the *Privacy Act* on a regular basis, in light of new technologies or government measures that may impact on the right to privacy of Canadians.

By contrast, PIPEDA requires that the first part of that Act be reviewed every five years. A number of provinces have a similar requirement for regular legislative review of their public sector privacy law.

What difference would it make?

A five-year review requirement would help synchronize the Canadian data protection framework across jurisdictions. It would also keep the privacy practices of both private and public sector organizations on the minds of Canadian decision-makers and industry. Finally, it would ensure federal law keeps pace with rapidly evolving technologies and international trends.

10 Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.

Background

Technological advances have made it much easier and less expensive for governments to collect and retain personal information about citizens. At the same time, information sharing between nations has increased dramatically as governments have adopted more coordinated approaches to regulating the movement of goods and people and to combating trans-national crimes and international terrorism.

For example, the Canadian Border Services Agency shares customs information and information about travellers entering Canada with other countries, while the Financial Transaction and Reports Analysis Centre (FINTRAC) has over 40 agreements with other financial intelligence units to share information about suspected money launderers and terrorists.

The *Privacy Act* does not reflect this increase in international information sharing. It places only two restrictions on disclosures to foreign governments: an agreement or arrangement must exist; and the personal information must be used for administering or enforcing a law or conducting an investigation.

The *Privacy Act* does not even require that an information-sharing arrangement be in writing, let alone impose any requirements concerning the content of such agreements.

The consequences of sharing personal information without adequate controls were dramatically highlighted in the Maher Arar case.

During the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Justice O'Connor concluded it was very likely that, in making the decisions to detain and remove Mr. Arar to Syria, U.S. authorities relied on inaccurate information about Mr. Arar provided by the RCMP. Justice O'Connor made a series of recommendations to strengthen RCMP policies and practices when sharing information with other government authorities.

The Government of Canada and Parliament should consider specific provisions to define the responsibilities of those transferring personal information to other jurisdictions and to address the adequacy of protection in those jurisdictions.

What difference would it make?

Good controls on information sharing would minimize the risks to Canadians. Better control would serve to ensure that information being shared is relevant and accurate,

that appropriate caveats are given, circumscribing the use of the information only for the purpose for which it was shared.

Conclusion

These 10 straightforward changes would begin the process of aligning the *Privacy Act* with modern data protection legislation around the world.

Our Office hopes that Canada will one day regain the leadership role in privacy promotion and protection it once held, when the *Privacy Act* was first adopted some 25 years ago.



PROACTIVELY SUPPORTING PARLIAMENT

A key part of the OPC's mandate under the Privacy Act is to support Parliament's work by providing information and advice on privacy issues

National security initiatives continued to raise privacy concerns in 2007-2008 and were a key focus of our work with Parliamentarians and officials in many government departments.

National security issues of particular note were Canada's new no-fly list, the government's lawful access consultations and plans for enhanced driver's licences in some provinces.

From our Office's point of view, one of the bright spots in the area of law enforcement was the introduction of legislation aimed at tackling identity theft.

The OPC also provided input on a number of other issues during the year, including possible amendments to copyright legislation and the development of electronic health records.

LAW ENFORCEMENT AND NATIONAL SECURITY INITIATIVES

It is impossible to overstate how privacy rights around the world have been rolled back since the terrorist attacks of Sept. 11, 2001. Governments everywhere – Canada included – have responded with a wide range of national security initiatives, which often focus on gathering more and more information about the routine, day-to-day activities of ordinary people.

Governments appear to believe that the key to national security and public safety is collecting, sorting and analysing mountains of personal data – without demonstrating the effectiveness of doing so.

Privacy often receives short shrift as new anti-terrorism and law enforcement initiatives are rolled out. This trend continues several years after the 9-11 tragedies.

Canadians expect the government to take measures to protect them; equally, they expect these measures will respect their rights, including their right to privacy, and also conform to the rule of law. This includes legal standards, such as due process, the right to consult counsel, the right to see evidence held against you and other elements of procedural fairness that underpin our justice system.

Privacy often receives short shrift as new anti-terrorism and law enforcement initiatives are rolled out. This trend continues several years after the 9-11 tragedies.

The following is a summary of some of the top national security and law enforcement issues of 2007-2008:

No-Fly List

Much of the post 9-11 focus has been on air travel security. In Canada, the federal government created a no-fly list which raises profound concerns about not only privacy, but other related human rights, such as freedom of association and expression and the right to mobility.

Fundamental flaws in the program were highlighted within days of the no-fly list, or Passenger Protect Program, coming into force in June 2007.

Two Canadian boys with the same name became entangled by North America's no-fly lists because they share the name of someone on one of these lists.

Their stories were similar: Alarm bells went off when each boy arrived at an airline check-in counter to try to catch a flight. The boys' families were told there was a security issue because of a name match with a no-fly list. (It was unclear which list they were on.) Both boys were allowed to fly after lengthy delays, apparently because their ages – 10 and 15 – made it clear they posed no threat.

An airline official warned one of the families there would be trouble each time their son tried to fly in the future and proposed a dramatic solution – changing his name.

The Passenger Protect Program involves the secretive use of personal information and, despite this significant intrusion on our privacy rights, Canadians have no legally enforceable rights to independent adjudication, compensation for out-of-pocket

expenses or other damages, or to appeal. Canadians also have no right to ask whether they are even on the list.

The government has said the list includes up to 2,000 names. There is clearly a significant risk for false positives – a problem we have seen in the US, where children and public figures such as Senator Edward Kennedy have faced questioning or been denied boarding.

Our Office has been clear that it will not stand in the way of initiatives which will protect the lives of Canadians. However, despite our repeated requests, Transport Canada has provided no evidence demonstrating the effectiveness of no-fly lists.

Some security experts suggest that improving physical screening at our airports – including thorough luggage and cargo checks – would be a more realistic and effective way to enhance aviation security.

An audit of the privacy management practices of the Passenger Protect Program is planned.

Shortly after the no-fly list came into effect, Canada's federal, provincial and territorial privacy commissioners and ombudsmen united to call for extensive reforms to the program. In a joint resolution, we called for the program to be suspended, or, at a minimum, to operate under strict ministerial scrutiny with regular public reports to Parliament while a comprehensive public Parliamentary review is completed.

NOTE: Information about our review of the Privacy Impact Assessment of the Passenger Protect program is included on page 82.

Privacy officials around the world share similar concerns about the widespread use of no-fly lists, as well as the collection and sharing of passenger data.

Data protection authorities attending the 29th International Conference of Data Protection and Privacy Commissioners in Montreal hosted by our Office supported a resolution calling for international standards for the use and disclosure of personal information collected by a travel carrier about its passengers.

The no-fly list was also a major focus when the Privacy Commissioner appeared before the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 in November 2007. We urged the Inquiry to consider the need for clear legal remedies, enforceable safeguards, and effective oversight as it assesses the adequacy of air travel security measures.

Lawful Access

In October 2007, Public Safety Canada issued a brief consultation paper on lawful access and difficulties faced by law enforcement agencies in obtaining customer information such as name, address, telephone number or IP address from telecommunications service providers.

Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation.

The Public Safety Canada consultation document says this is making the job of police officers challenging because they may have no means to compel the organizations to provide the information they are seeking.

“For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation,” the consultation paper said.

The consultation document does not provide any sense of the scope of the difficulties mentioned in the document. Are 20 per cent or 80 per cent of companies providing information voluntarily? Do companies respond differently depending on the situation – in a next-of-kin emergency situation versus a request involving suspected violent crimes? We don’t have the answers to these key questions.

In our Office’s opinion, requiring all telecommunications service providers to disclose customer information on request is an overly broad, one-size-fits-all response to a problem that has not been clearly defined or measured.

Neither this consultation paper, nor previous consultation documents has presented a compelling case based on empirical evidence that the inability to obtain customer data in a timely way has created serious problems for law enforcement and national security agencies.

Assuming there is a well-documented and empirically demonstrated problem in obtaining access to customer information, we are not convinced that requiring telecommunications service providers to disclose this information without a warrant is the only, or most appropriate, solution.

It is our view that there is a reasonable expectation of privacy in customer data – making any mandatory disclosures or seizures of dubious constitutional validity.

Although the consultation paper identified the “absence of explicit legislation” as a problem to be addressed, PIPEDA is, in fact, an explicit legislative code which permits lawful access by law enforcement and national security agencies while protecting the privacy and other rights and freedoms of Canadians.

PIPEDA allows telecommunications service providers and other organizations to disclose personal information without consent to law enforcement agencies without a warrant for the purpose of enforcing a law or carrying out an investigation. It also allows disclosures without consent in emergencies which threaten someone’s life, health or security.

Lawful access was the subject of considerable discussion during a five-year review of PIPEDA conducted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics. In its response, the government indicated there is a need to clarify the concept of lawful authority. The government noted that PIPEDA currently allows organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order.

Before considering legislation which would make the disclosure of customer information mandatory on request, we would strongly recommend that the government determine whether clarification to PIPEDA, together with any guidance that may be appropriate, could address the perceived problem.

Lawful access raises fundamental issues for rights such as privacy and the ability to communicate freely. Our Office will continue to monitor this issue and to raise our concerns with government officials and Parliamentarians.

Enhanced Driver’s Licences

Plans to consider or implement enhanced driver’s licences (EDLs) in several Canadian provinces have prompted our Office as well as provincial and territorial privacy guardians to express their concerns about privacy and security risks.

The moves toward enhanced driver’s licences are a provincial response to the U.S. government’s requirement that travellers provide proof of identity and citizenship to comply with the Western Hemisphere Travel Initiative.

These developments have raised concerns among federal, provincial and territorial commissioners and ombudsmen responsible for privacy.

A key concern is that personal information of participating drivers should remain in Canada and that there is meaningful and independent oversight of how the U.S. Customs and Border Protection receives and uses Canadians’ personal information.

As well, RFID technology in enhanced driver's licences poses a potential privacy threat because it may permit the surreptitious location tracking of individuals carrying an EDL. The technology may not encrypt or otherwise protect the unique identifying number assigned to the holder of the EDL and would not protect any other personal information stored on the RFID.

In February 2008, we issued a unanimous joint resolution outlining the steps that will need to be taken to ensure the privacy and security of any Canadian's personal information accessed as part of EDL programs.

In the resolution, we emphasized that Canadian citizens already have access to a well-established, highly-secure travel identification document in the form of the Canadian passport, but acknowledged that some may want an alternative.

Identity Theft

New legislation aimed at addressing identity theft represents a significant step forward in tackling this growing crime.

A central notion of privacy is that people should be able to control how, when and for what purposes their personal information is used. Victims of identity theft have clearly lost control over their personal information – with often serious and long-lasting consequences. Their privacy has been violated in a very significant way.

Identity theft is a complex problem, with many contributing factors.

Bill C-27 focused on the early stages of identity theft and addressed a number of different ways in which criminals gather personal information. For example, it:

- Makes it an offence to possess or traffic in identity information when this information is to be used for a fraudulent purpose;
- Tackles a common technique used by identity thieves – mail re-direction – by making it an offence to fraudulently redirect anything sent by post; and possess a mail key;
- Addresses credit card fraud by creating a new offence dealing with the possession of instruments for copying credit card information; and
- Makes the obtaining, selling or possessing of “identity documents” that relate to another person an offence, punishable by up to five years in prison.

These changes will provide police officers with important new tools to stop identity thieves or fraudsters *before* Canadians suffer actual financial harm.

Another praiseworthy element of the legislation is the possibility that offenders will be required to pay restitution to victims. This is significant in that it recognizes the serious financial impact identity theft can have on individuals.

It is our view, however, that this identity theft bill is only a beginning and that other types of legislative changes are also necessary.

For example, a key issue not addressed in Bill C-27 is pretexting – where an individual obtains personal information, such as telephone or financial records, by pretending to be someone authorized to have it. We also need to legislate against spam – often used by identity thieves to trick people into providing personal information online. Canada is the only G-8 country without anti-spam legislation.

OTHER LEGISLATION AND INITIATIVES WITH AN IMPACT ON PRIVACY

Copyright

The federal government has been studying changes to the *Copyright Act* for the last few years.

In January 2008, the Privacy Commissioner wrote to the Minister of Industry and the Minister of Canadian Heritage regarding possible amendments to the Act.

In particular, our Office is concerned about possible changes authorizing the use of technical mechanisms to prevent copyright infringement that could have a negative impact on the privacy rights of Canadians. In some cases, such mechanisms to protect copyrighted material result in the collection, use and disclosure of personal information without consent.

Technological protective measures can be embedded in various media to control copying and prevent copyright infringement, or they can be built into electronic devices to prevent the reading of unauthorized content.

Digital rights management is the general term for the varied technologies used to enforce pre-defined limitations on the use of digital content. These include any means by which publishers or manufacturers control use of data or hardware.

If digital rights management technologies only controlled copying and use of content, we would have few concerns. However, they can still collect detailed personal information from users, who often access the content on a computer. This information is transmitted back to the copyright owner or content provider, without the consent or knowledge of the user.

Although the means exist to circumvent these technologies and thus prevent the collection of this information, previous proposals to amend the *Copyright Act* contained anti-circumvention provisions.

Technologies that report back to a company about the use of a product reveal a great deal about an individual's tastes and preferences. Indeed, such information can be extremely personal.

Our Office will carefully assess the privacy implications of any legislation to amend the *Copyright Act*.

Electronic health records

The federal government is encouraging the development of a system of electronic health records through the Federal Healthcare Partnership.

We are monitoring the progress of this group, which would impact the health care services provided to First Nations and Inuit populations, eligible veterans, members of the Canadian Forces, RCMP, federal inmates and refugee protection claimants.

As well, our Office is an active participant in the new Canada Health Infoway Privacy Forum, which brings together representatives of the health ministries and privacy oversight offices across Canada. The Forum is discussing fundamental privacy and governance issues that must be addressed to ensure the successful implementation of electronic health records.

Infoway's goal is to ensure that, by 2010, half of Canadians will have their electronic health record readily available to health care providers.

While electronic health records offer significant benefits, such as rapid access to complete patient information for health professionals, they also raise a number of privacy risks.

The protection of privacy must be a key factor as we consider how these highly sensitive records are managed. It is crucial that patients know what is happening to their health information and feel confident that they can exercise a measure of control over it.

Electronic health records will require extremely strong security measures, including safeguards to ensure only authorized people can access the information. Careful attention must also be given to potential secondary uses for the information, including health research.

RESPONDING TO COMPLAINTS AND PRIVACY INCIDENTS

How the OPC dealt with complaints and incidents under the Privacy Act in 2007-2008

The complaints we receive show Canadians have a wide range of concerns about how the government is handling their personal information.

Canadians are uneasy about the sharing of information between departments; the use of e-mail to record and/or share information; and the problems associated with institutions maintaining and properly allowing individuals a right of access to personal information stored on computers.

We have also noticed a growing concern about how government institutions are protecting their information. Headlines about personal information being lost or stolen when public servants telework or bring home work on laptops do not inspire public confidence.

The cases we investigated over the year also highlighted how human error can jeopardize personal privacy. Some of the breaches we looked at show how problems with computers and use of other mechanized equipment designed to improve government processes can result in the disclosure of personal information. It is also clear that government institutions must continue to emphasize to employees the importance of safeguarding personal information and privacy.

Another issue which continues to concern our Office is ongoing delays in processing individuals' requests for access to their personal information. While some departments have improved their response times, many federal Access to Information and Privacy (ATIP) units are overwhelmed.

NOTE: Detailed statistical charts; definitions of each type of complaint and findings; and a chart describing the course of a *Privacy Act* investigation are included in the Appendices.

Snapshot: Inquiries, Complaints and Investigations

Inquiries

<i>Privacy Act</i> inquiries received:	4,258
General privacy inquiries:	2,367
Total (excludes PIPEDA inquiries):	6,625

Complaints

Total new complaints received:	759
--------------------------------	-----

Top 10 institutions by complaints received

Correctional Service Canada	248
Royal Canadian Mounted Police	84
Canada Border Services Agency	54
Service Canada	52
National Defence	48
Canadian Security Intelligence Service	45
Canada Revenue Agency	38
Canada Post Corporation	28
Foreign Affairs and International Trade	27
Justice Canada	18
Others	117
Total	759

Inquiries

Our Office received a total of 4,258 inquiries related to the *Privacy Act* and another 2,367 more general inquiries about privacy in 2007-2008. These figures do not include the 7,636 inquiries related to PIPEDA, the legislation applying to the private sector, received in 2007. The average daily number of inquiries we receive about all privacy issues is close to 60.

Our inquiries unit provides an extremely important service to Canadians, who are able to obtain a timely response to questions touching on a wide array of privacy issues.

Our inquiries unit provides an extremely important service to Canadians, who are able to obtain a timely response to questions touching on a wide array of privacy issues.

Complaints

We received 759 new complaints, down slightly from the previous year's 839.

The number of complaints filed against institutions does not necessarily mean that these institutions are not compliant with the *Privacy Act*.

Some institutions – because of their mandate – hold a substantial amount of personal information and are more likely to receive numerous requests for access to that information. There is also a higher likelihood of complaints about the institution's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

Correctional Service Canada and the RCMP have been the top two institutions receiving complaints over the past few years. It is noteworthy that there has been a steady drop in the number of RCMP complaints, but a fairly significant increase in Correctional Service Canada complaints – from 190 in 2005-2006 to 248 in 2007-2008. The rise in the number of complaints against Correctional Services Canada may be directly proportional to the additional access to personal information requests it received.

A complete list of complaints received by institution can be found in Appendix 3.

The majority of all new complaints were from individuals who claimed that federal government institutions denied them a right of access to their personal information. The second most common type concerned the 30-day statutory time limit (extended to 60 days in some circumstances) for institutions to respond to a personal information request.

Detailed information about complaints received by type can be found in Appendix 3.

Closed Complaints in 2007-2008

Total	880
--------------	------------

Top 3 Categories of Closed Complaints

Denial of access	318
Time Limits Exceeded	301
Improper use / disclosure of personal information	134

Disposition of Closed Complaints

Discontinued	117
Early resolution	32
Settled during the course of investigation	114
Resolved	6
Not well-founded	275
Well-founded	319
Well-founded and resolved	17
Total	880

Individuals may discontinue their complaints because they have resolved the issue with the institution before the active investigation has begun. Our Office may also discontinue complaints due to a lack of information necessary to complete our investigations. When a complaint is resolved through early resolution or by settling, this indicates the individual is satisfied with the actions taken by the institution as a result of our intervention.

Obtaining Access to Personal Information

Obtaining access to personal information held by a government institution is a basic privacy right that is afforded to individuals under the *Privacy Act*. However, it is clear many Canadians are having difficulties exercising this right. More than 70 per cent of the complaints filed with this Office related to individuals expressing concern about being denied access to their personal information or because institutions failed to provide that information within the statutory time limit.

Our Office is pleased to see that the total number of complaints in both these categories has declined over the last few years. This may be because individuals are dealing directly with institutions to resolve their concerns, a practice that our Office encourages.

Time limit complaints are opened when an individual notifies this Office that an institution has failed to respond to his or her *Privacy Act* request within 30 days. In some cases a year had passed without the institutions responding to individuals' requests. One complainant had been waiting for more than two years for a response to his request.

Investigations and Inquiries Challenges

Our Office is facing its own challenges in responding to complaints in a timely way. We are strongly committed to improving our complaint treatment times.

In 2007-2008, we received 759 complaints and closed 880. We had a backlog of 370 complaints that were unassigned because of a lack of investigators. On average, it took 14.5 months to complete a complaint investigation. We know this is unacceptable and are undertaking a number of measures to remedy the situation.

A detailed breakdown of the treatment times by finding and complaint type can be found in Appendix 3.

We are challenged by the fact that, under the wording of the *Privacy Act*, we need to deal with every complaint we receive. Other data protection authorities around the world and in Canadian provinces are also finding similar challenges with the need to address all complaints received – regardless of their nature or seriousness.

Our Office has asked the federal government for legislative amendments to provide us with this flexibility, a step that would allow us to better focus our investigative resources. (See page 45 for more detailed information.)

Another major challenge is attracting and retaining seasoned investigators and managers in this area. People with *Privacy Act* and investigation experience are in high demand across government and there are not enough qualified individuals to go around. An older generation is retiring and the new generation is extremely mobile in a competitive job market. Turnover rates in this area have been higher than elsewhere in the OPC due to retirement and external demand.

We are continuing to revitalize our investigations unit by focusing our efforts on recruitment, as well as looking at innovative means to improve service delivery to Canadians.

Our strategy includes re-engineering our investigative process by streamlining inquiries, complaints and investigations. We will triage complaints and identify those which could likely be resolved early in the process. A new case-management system will help us to better identify trends and focus resources where they can have the most impact.

We anticipate it will take a year to build capacity, diminish the backlog, continue hiring and training more staff to investigate in innovative ways. Our goal is to complete the re-engineering initiative in the spring of 2009.

Training and Inter-jurisdictional Cooperation

Training will play an important role in our continuous efforts to improve how we investigate and attempt to resolve complaints about privacy breaches.

In February 2008, we hosted our fourth annual investigators conference. We welcomed more than 90 participants at this Ottawa event, including representatives from 12 of the 13 provincial and territorial privacy offices, and, for the first time, members of the Office of the Information Commissioner of Canada. The conference allowed investigators to share experiences and best practices. Open and frank discussions increased awareness of common issues.

Complaints – Examples of Cases the OPC Investigated

Passport Canada apologizes for “unacceptable error”

The complainant mailed his passport renewal application to Passport Canada. As required, he provided his expiring passport, photocopies of his driver's licence and health card, and his original birth certificate. When he received his new passport in the mail, the envelope contained another person's expired passport and other personal documents.

The individual notified Passport Canada of the error. The agency asked him to return the other individual's documents, which he did, and said that it would search for his documents. Passport Canada contacted the other individual and learned that he had destroyed the complainant's documents.

Our investigation determined that a passport employee had mixed up the contents of two files and then failed to check that the labelled envelope, new passport and other documents all matched the intended recipient.

Passport Canada apologized for what it acknowledged was an “unacceptable error” and said it had taken steps to ensure it did not happen again. Managers now hold monthly briefings with staff to verify that proper procedures are being followed. In addition, the agency posts the procedures and all new employees are trained and instructed on the importance of verifying documentation prior to it being placed in an envelope and mailed to a recipient.

The complaint was well-founded.

Inmate report discovered in prison gym garbage can

A report containing pictures, names, birthdates and cell locations of 96 inmates, as well as other personal information, was found in an offender's cell at an Alberta prison. Fourteen affected inmates complained to our Office.

An offender had discovered the report in a garbage can in the prison's gym. Correctional Service Canada's investigation determined that this report was routinely updated and posted for correctional officers in an office next to the gym. Out-of-date reports were being regularly discarded in the gym's garbage can.

To ensure that such a disclosure does not occur again, Correctional Service Canada instructed the institution to stop posting this type of information in the office next to an area used by offenders and to take greater care with personal information.

The complaint was well-founded.

Canada Revenue Agency employee misuses information

A woman complained that her former neighbour, who worked for the Canada Revenue Agency, improperly gained access to her tax files in order to identify her place of employment and then used this information to make harassing and threatening phone calls.

The complainant had a history of problems with the Canada Revenue Agency employee. She stated that the employee and her family had threatened and harassed her for years. The complainant moved and obtained an unlisted telephone number. After her move, she began receiving harassing calls at her place of work. She determined that these originated from the Canada Revenue Agency employee.

The agency confirmed that its employee had used her position to gain access to the complainant's personal information. This included the complainant's address, Social Insurance Number, place of employment, income and deductions. The agency confronted the employee about her actions and she confirmed she had viewed the complainant's tax information. She was disciplined for the unauthorized access to the complainant's personal information.

The CRA has an extensive audit trail process allowing it to maintain the security of taxpayers' information.

The complaint was well-founded.

Identity of information requester revealed

A Foreign Affairs and International Trade Canada (DFAIT) employee complained the institution improperly disclosed his personal information to co-workers. The co-workers then disclosed it to the Public Service Alliance of Canada.

In addition to being a DFAIT employee, the complainant's union work had been criticized by the local's executive and some members. The complainant submitted *Privacy Act* requests seeking all personal information held by five co-workers, who were also his fellow union members and the ones who had criticized him.

When DFAIT received his requests, the ATIP unit asked the co-workers to provide all personal information they held about the complainant. ATIP staff alerted the co-workers of the sensitivity of the request and informed them of the restriction for further dissemination of that information on a "need-to-know" basis within the institution.

The first issue our Office reviewed was the complainant's concern about being identified as the requester. We concluded this complaint was not well-founded. In order to obtain the information held by the co-workers, the ATIP unit needed to disclose his identity.

As for the complainant's concern about the co-workers notifying the union that he had submitted *Privacy Act* requests, our investigation confirmed that four of the five had informed the Public Service Alliance of Canada of his actions. The co-workers believed that the complainant had submitted his requests in an effort to harass them. All four confirmed they had read the ATIP unit's reminder about the sensitivity of his request, but considered the matter union business, not departmental business.

While the disclosure of the complainant's identity to his co-workers was not well-founded, the fact that four co-workers notified the union that he had submitted *Privacy Act* requests violated his privacy rights.

The complaint was well-founded.

Monitoring of employee's e-mails was appropriate

An Indian and Northern Affairs employee complained that the institution did not have the authority to restore 35 months of the employee's e-mails and then review all of the messages contained in the departmental account. The employee alleged that as a result of the department's actions, the employee's personal information was improperly accessed.

The employee was the subject of an administrative investigation into allegations that the employee was misusing the department's network.

During the course of its investigation into the complainant's actions, the institution restored the complainant's e-mail account and found pornographic e-mails.

Later, the employee received a copy of the Terms of Reference for the administrative investigation and noted that it was not signed. The employee contended that, as the document was not signed, the institution had no authority to restore or read the e-mails. The employee also contended that there should have been notification of the institution's actions.

Treasury Board's policy states that if an institution reasonably suspects that an individual is misusing a department's network it must refer the matter for further investigation and action which may involve special monitoring and/or reading the contents of an individual's e-mails.

Indian and Northern Affairs policy states that management is permitted to have access to an employee's e-mail in the course of any investigation relating to impropriety, security breaches, violation of a law or infringement of departmental policies.

Although the Terms of Reference were not signed and the employee was not advised of the institution's actions, Indian and Northern Affairs did not violate Treasury Board's policy on network use or the employee's privacy rights. Under the *Privacy Act*, institutions may use personal information for the purpose for which it was obtained or compiled or for a use consistent with that purpose. In this case, the information gathered from the employee's e-mail account was used solely for the purpose of the institution's administrative investigation.

The complaint was not well-founded.

Reporter identified in response to access request

A journalist complained that his name had been improperly released in a response to a request made under the *Access to Information Act* (ATIA). The name of the journalist appeared in an e-mail message prepared by a Privy Council Office employee.

The e-mail came to light after another reporter requested access to all e-mails and communications sent or received by the director of communications in the Prime Minister's Office.

The response to that request included an e-mail from an employee of the Privy Council Office (PCO) to 19 government officials in both the PCO and the Prime Minister's Office.

The e-mail was written after a multi-department conference call during which an official with Public Safety Canada discussed the pending release of information about a sensitive issue in response to an ATI request. In the e-mail, the PCO official discussed the possibility of another article being written by the complainant about a sensitive issue that he had previously reported on. Other reporters' names were also mentioned in the e-mail, primarily concerning stories that had already appeared in print. While their names were blacked out, the complainant's name had been overlooked and released in error.

The Privy Council Office subsequently apologized to the complainant.

As the complainant's name was released to the other reporter in response to an ATI request, the OPC concluded that his privacy rights had been violated. The complaint was well-founded.

A related complaint alleged that the PCO official disclosed that the journalist had filed an ATI request to Public Safety Canada during the multi-department conference call.

However, our investigation confirmed that the ATI requestor's identity was never disclosed outside of the ATIP office of Public Safety Canada.

The PCO official stated he had simply made an assumption about who had made the request based on the fact that the journalist had written a number of articles on the subject.

The Assistant Commissioner was satisfied that the journalist's identity as the person making the access request was not under the control of PCO. This complaint was not well-founded.

A third complaint from the same journalist against Public Safety Canada that it had disclosed his name as an ATI requester was also not well-founded. That complaint was closed in the previous reporting year.

Improper disclosure of information to prospective employer

A man contended that Human Resources and Skills Development Canada (HRSDC, now Service Canada) improperly provided his Social Insurance Number, address, birth date, income information and employment insurance application details to a prospective employer.

While receiving employment insurance (EI) benefits, the complainant turned down a job offer from a company. As a result, HRSDC disqualified his EI benefits. The

complainant appealed its decision to the Board of Referees. He claimed that he had refused the job because of working conditions.

In accordance with the *Employment Insurance Act*, when an individual appeals a decision to the Board of Referees, HRSDC may share that individual's information with interested parties such as employers and any person with a vested interest. The disclosure of information to these parties is necessary to establish the validity of an individual's request for continuation of EI benefits.

In this case, HRSDC deemed that the prospective employer was a party to the complainant's appeal and gave the company a complete package of information. HRSDC did not review the complainant's file and released his Social Insurance Number, birth date and information relating to his past employment record, including rates of pay and overtime. As the complainant's appeal to the Board of Referees was based on refusing the job offer because of working conditions, the information released by HRSDC to the parties should have been limited to what was required to establish the validity of his decision to refuse that job offer.

HRSDC agreed that it had released too much information, calling the incident an "honest mistake made in good faith by an employee." As a result of this complaint, it reviewed its policies and procedures and changed the definition of employer to include "a current or former person or organization for whom the claimant worked." A prospective or potential employer is no longer considered an interested party in the appeal process.

The complaint was well-founded.

Incidents under the *Privacy Act*

Our Office also reviews cases involving the mismanagement of personal information which come to our attention through media reports, affected individuals or breach notifications from government institutions.

Data breaches

Treasury Board Secretariat published privacy breach guidelines for institutions subject to the *Privacy Act* at the end of March 2007. The guidelines "strongly recommend" that government institutions notify the OPC if a breach involves sensitive personal information such as financial or medical information or Social Insurance Numbers or if there is a risk of identity theft or some other harm or embarrassment which could have an impact on an individual's reputation, financial position or safety.

During the first year in which the guidelines have been in place, we have noticed an increase in the number of reported incidents (57 in 2007-2008 as compared to 43 for 2006-2007). The fact that the number of incidents is relatively low, when one considers the large amount of personal information held by government institutions, is encouraging news.

Most incidents occurred as a result of human error or theft, for example, when documents containing someone's personal information were lost, or when a government employee's briefcase was stolen from a hotel room or a laptop was taken from a vehicle. In one instance, employees gained unauthorized access to personal information stored on government computer systems.

The following are some typical incidents we reviewed:

Technology glitch results in disclosure of sensitive information

A failed effort by Public Works and Government Services Canada (PWGSC) to remove exempted information when it respond to *Access to Information Act* (ATIA) requests using CDs rather than paper format compromised a number of individuals' personal information.

Over the last number of years, institutions have been responding to some *Access to Information Act* and *Privacy Act* requests by sending the information on CDs rather than in paper format. At PWGSC, the CDs were scanned in "Tagged Image File Format" (TIFF), which is a picture copy of the document. The imaging program was changed to "Portable Document Format" (PDF) when requesters complained about having difficulties in opening TIFF files.

The recipient of one of the CDs that contained the information in PDF format informed the institution he was able to read the information that had been exempted. He said that he simply selected the severed portions and pasted them into another document.

Before this problem was brought to its attention, the institution had responded to 123 ATIA requests and one *Privacy Act* request using the PDF format. As a result, people who received the CDs were able to read the names and home addresses of government employees being investigated for fraud involving government credit cards, the names and birth dates of people undergoing security clearances, the results of second language evaluations and employee leave information.

In an effort to minimize any further disclosure, PWGSC attempted to retrieve the CDs from requesters. Some requesters did return the CDs, while others said they had

destroyed or lost them. Individuals whose personal information was at risk were notified by the institution of the potential breach.

It was determined that the problem was a flaw in an imaging system. The manufacturer of the software was contacted and confirmed that PWGSC was the only institution with a flawed version. That being said, to ensure that this did not occur in another institution, Treasury Board prepared a general security bulletin warning institutions not to release information on CDs until they received certification that their programs were secure.

Stolen laptop contains household survey information

An encrypted laptop stolen from a Statistics Canada employee's home contained the personal information of several Canadians who had taken part in surveys. Unfortunately, the employee had written down the two passwords required to access the laptop's information on a Post-it note stored in the computer's case.

The laptop contained a total of six Labour Force Survey and Canadian Community Health Survey cases. The labour surveys contained contact information, household information, rent, employment and income and demographic information, while the health surveys contained highly sensitive personal information including height, weight, sleep patterns, sexual behaviours, chronic conditions, stress, use of tobacco and alcohol, illicit drug use and mental health information.

The employee immediately reported the theft to police. Statistics Canada officials visited each of the affected households and informed the residents that their personal information had been compromised.

The department addressed the issue in an appropriate manner with the employee whose laptop was stolen. The department also sent out a newsletter to all field employees reminding them of their obligations to secure laptops and control the use of their passwords, user identification, and computer accounts. Our Office was satisfied with the measures implemented by Statistics Canada.

Human error compromises taxpayers' information

After using the Canada Revenue Agency's telephone service to inquire about information related to his Registered Retirement Savings Plan, an individual received an envelope containing the Notices of Assessment of nine other taxpayers.

The man called the agency to report the problem, but had trouble communicating with the telephone agent. He asked to speak to a supervisor, but was initially refused. A supervisor called back, asking him to return the documents. The man was left with

the impression that the agency was not taking the matter seriously and contacted two television stations.

Camera crews recorded the man personally returning a Notice of Assessment to one individual who lived nearby and bringing the other documents to a Canada Revenue Agency office.

Following the incident, Canada Revenue Agency reviewed its procedures and policies involving documents prepared for faxing and mailing and made corrections. The agency also apologized to the affected taxpayers.

Our Office concluded the incident was the result of human error.

Failure to reset envelope-stuffing machine leads to privacy breach

An employee of a private company which administers the Veterans Independence Program for Veterans Affairs Canada forgot to reset an automated envelope stuffing machine, a mistake which meant 122 cheques were double-stuffed into 61 envelopes.

The company investigated the incident and put in place a new quality assurance system. It now documents the number of cheques handled each day and it reconciles the number of cheques printed against the number of envelopes prior to their mail-out. Any discrepancies in the numbers will result in immediate investigation and correction. In addition, it implemented a policy whereby it now individually stuffs envelopes containing reimbursement cheques.

Veterans Affairs Canada telephoned the affected veterans to check on the status of their cheques, and the company sent out apology letters. Cheques were either redirected to the proper recipients or new cheques were issued.

Our Office reviewed Veterans Affairs' report on this incident and was satisfied with the action it took to notify the affected individuals and the measures it implemented to ensure that this type of error isn't repeated.

Public Interest Disclosures under the *Privacy Act*

When there is a compelling public interest that outweighs an individual's personal privacy, the heads of government institutions may, under the *Privacy Act*, use their discretion to disclose personal information without an individual's consent.

Unless the situation that arises is an emergency, institutions disclosing personal information in the public interest must notify the Privacy Commissioner in advance.

After reviewing the proposed disclosure, the Commissioner may, if she deems it necessary, notify an individual of the release of his or her personal information. The OPC will also recommend ways to minimize the amount of personal information being disclosed if we feel a department's proposal to release personal information goes beyond the public interest.

In 2007-2008, our Office reviewed 83 public interest disclosure notices. Most were from the RCMP and involved high-risk offenders being released from prison and who police believed were a danger to the community. In other instances, the RCMP released personal information to the public in order to locate suspects or provide a warning about the actions of a violent or sexual offender.

In other cases, the Department of National Defence and Correctional Service Canada released information about the death of individuals to family members. Information about the nature of those deaths is provided for compassionate reasons.

Other Examples of Public Interest Disclosures

Tuberculosis scare prompts identification of passenger

The Department of Foreign Affairs and International Trade informed our Office it had released to the Public Health Agency of Canada the identities and contact information for 27 people who had been seated close to an airline passenger with infectious tuberculosis for more than eight hours during an international flight.

The Public Health Agency was then able to contact passengers from the flight to advise them of the need to be tested for tuberculosis.

In this case, the disclosure in the public interest clearly outweighed any potential invasion of an individual's privacy.

Auditor General identifies Quebec's Lieutenant Governor's misuse of funds

The Office of the Auditor General of Canada informed our Office that it intended to release personal information about the Lieutenant Governor of Quebec's improper use of federal public funds.

The Auditor General based her decision on the opinion that releasing the information was in the public interest. Our Office concluded no further action was necessary.

Military Ombudsman releases report about Canadian Forces snipers

The office of the National Defence and Canadian Forces Ombudsman informed our Office that it intended to release a report entitled: *A Sniper's Battle – A Father's Concern – An Investigation into the Treatment of a Canadian Forces Sniper Deployed to Afghanistan in 2002 – Special Report to the Minister of National Defence and the Chief of the National Defence Staff*.

The report concerned allegations made by the father of one of six officers in a sniper unit. He alleged the officers were ostracized, treated unfairly, denied stress debriefings and subjected to unfounded criminal and other investigations.

Two individuals named in the report consented to the release of their personal information. The Ombudsman believed it was possible to identify other individuals mentioned, but not named. However, he believed that disclosing the report was in the public interest and outweighed any invasion of privacy.

The Ombudsman's office notified four people about the report's impending release and gave them each a copy. The OPC reviewed the matter and recommended the Ombudsman's Office inform the two other individuals about the report's release and the possibility they could be identified. The Ombudsman's office agreed.

Complaints Commission report reveals personal information

The Military Police Complaints Commission is an independent federal body that oversees and reviews complaints of conduct of members of the Military Police.

The Complaints Commission received a complaint from a member of a sniper unit deployed to Afghanistan expressing concern about the conduct of the Military Police. The Commission investigated the allegations made against the Military Police and notified the OPC that it intended to disclose personal information contained in its report by posting it on its website. The Complaints Commission argued the report contained information crucial to the public interest.

The Commission had determined the allegations against military police officers were unfounded.

The complainants, the members of the Military Police, the Minister of National Defence and other departmental officials received copies of the report before it was posted, and were told it would be made public. Other individuals named in the report as having been interviewed during the investigation were not notified.

The OPC recommended that the Commission consider notifying the interviewees of its intention to render the report public. We also recommended that the Commission depersonalize the report to protect the identities of the parties and interviewees.

OTHER OPC ACTIVITIES

AUDIT AND REVIEW

Our Office's audit work resulted in our first special report to Parliament this year. Problems uncovered during an audit of the RCMP's exempt data banks raised such significant concerns that the Commissioner decided to present the findings in a special report tabled in February 2008.

We also completed a comprehensive examination of passport operations. (See page 15.)

Other issues our Audit and Review branch worked on over 2007-2008 included the government's purchase of personal information from data brokers and the widespread use of Social Insurance Numbers.

We also conducted reviews of Privacy Impact Assessments for new federal initiatives, offering hundreds of recommendations to help protect Canadians' privacy.

RCMP Exempt Databanks – A Special Report to Parliament

An OPC audit found the RCMP's exempt data banks, which shelter national security and criminal intelligence files from public access, have been crowded with tens of thousands of records that should not have been there. This conclusion is particularly disturbing given that the RCMP was advised of compliance problems 20 years ago and made a commitment to properly manage such banks.

Exempt data banks serve to withhold the most sensitive national security and criminal intelligence information. Departments and agencies controlling such records will refuse to confirm or deny the existence of information in response to requests for access.

People whose names appear in the RCMP's exempt data banks could be at risk of harmful impacts. For example, they could have trouble obtaining an employment security clearance or crossing the border.

More than half of the files examined as part of our audit did not belong in the exempt banks. To illustrate, one seven-year-old file in the national security exempt bank detailed a resident's tip that a man had gone into a rooming house and drugs might be involved. Police investigated, but found the man had simply dropped his daughter off at a nearby school and stepped out of his car to smoke.

The Privacy Commissioner was satisfied the RCMP was taking her recommendations seriously and would take action to ensure its exempt banks comply with the *Privacy Act* and RCMP policy. Our Office will conduct a post-audit.

The complete audit report is available on the OPC website.

Project Shock

The RCMP's National Security Investigations Records exempt bank includes records related to "Project Shock" — the effort to coordinate tips related to the 9-11 terrorist attacks.

We examined a sample of records in 2002 and found tips generally related to suspected terrorist affiliations, suspicious persons or suspicious activity. However, some tips seemed to amount to little more than public hysteria during a time of crisis.

While these files were not part of our exempt bank audit, we asked questions in order to verify that each tip file had undergone an assessment to determine whether it warranted continued exempt bank status.

As we reported in our special report, a subsequent RCMP review of the Project Shock file, which contained records that touch on thousands of Canadians, found the records did not meet the criteria for continued inclusion in the national security exempt bank and were removed.

Data Mining and the Public Sector

Concerns about how data brokers collect, use and disclose personal information have been on our radar screen for a number of years. As well, privacy concerns have been highlighted in a number of studies and high-profile incidents involving data brokers.

In late 2006, the *Ottawa Citizen* published an article describing how the RCMP had been buying and storing personal information from commercial data brokers for a number of years. This revelation raised questions not only about how the RCMP was using the information, but also about whether other government departments were purchasing data broker information.

Data brokers collect and analyze personal information – for example, financial, credit or health information – for the purpose of developing and selling data products, often to marketers. From a privacy perspective, we have concerns about the accuracy of this kind of data as well as the possibility that incorrect assumptions about individuals may be drawn.

The RCMP advised our Office that it has contractual agreements with a number of data brokers which provide commercial reports for public and private companies, and contact information (address and telephone numbers) for consumers and businesses.

The extent of data broker use within the RCMP varies depending on the mandate of the operational unit. For example, RCMP Commercial Crime Units may prepare economic profiles on individuals and companies in the course of bankruptcy investigations.

The RCMP told us that information from data brokers complements the force's intelligence and investigative work, and is only considered as a secondary source of information of unknown relevance, accuracy and reliability. We understand no action is undertaken solely on the basis of such information.

Our Office also conducted a limited survey to assess the use of data brokers by other federal government departments. We concluded the use of data brokers does not appear to be widespread.

Treasury Board Secretariat has told us that it will consider the data broker issue as it reviews the Treasury Board Privacy Impact Assessment Policy, which is scheduled to be completed by April 2009.

Use of Social Insurance Numbers

A senior citizen wrote to the Privacy Commissioner in June 2007 to express concern about the inclusion of Social Insurance Numbers on Old Age Security identification cards. The citizen pointed out that this was forcing older Canadians to reveal sensitive personal information each time they used the card to obtain privileges such as seniors' discounts.

The letter prompted our Office to contact Human Resources and Social Development Canada to raise the concerns. A few months later, the department informed us that Social Insurance Numbers would no longer be printed on the cards.

This Social Insurance Number was created in 1964 to serve as a client account number for the Canada Pension Plan and various employment insurance programs. In 1967, what is now Canada Revenue Agency (CRA) started using Social Insurance Numbers for tax reporting purposes.

A recent OPC study found that over 70 federal departments and agencies use Social Insurance Numbers in one way or another. Meanwhile, approximately 170 pieces of provincial legislation deal with uses of Social Insurance Numbers.

Despite the efforts of governments, our Office, other privacy commissioners, privacy advocates and citizens to limit the use of Social Insurance Numbers, over many years, the use of this number has snowballed to the point where many see it as a *de facto* common client identifier, if not a national identifier.

At the same time, there is no legislated privacy protection related to the use of Social Insurance Numbers. This is a significant concern given that a Social Insurance Number is a key piece of information to unlock the door to an individual's personal information. For example, identity thieves use it to apply for credit cards and open bank accounts.

Treasury Board Secretariat recently issued a new policy governing the use of Social Insurance Numbers and whether this helps curtail the use of this number remains to be seen.

Privacy Impact Assessment Reviews

Privacy Impact Assessments (PIAs) are an important privacy management tool to help federal government institutions identify and mitigate privacy risks before implementing programs.

PIAs – which are mandated by Treasury Board Secretariat policy – are meant to help departments focus on privacy as a core consideration when implementing new programs and initiatives. Our Office believes PIAs should be mandated under the *Privacy Act*. (See page 44 for more detailed information.)

The OPC's Audit and Review Branch reviews submitted PIAs to evaluate the privacy risks of government programs and services, and offers advice where appropriate. In this way, the OPC can ensure that privacy safeguards are built in to programs and systems.

PIAs by the Numbers

New PIAs sent to the OPC for review	60
PIAs reviewed and letters of recommendation sent to departments (includes PIAs received in prior years)	78
Recommendations made by OPC to departments	434
Requests made to departments for information missing from PIAs	239

Our Office was pleased to note that, increasingly, departments are inviting OPC officials to early consultation meetings during – or even before – the PIA development stage. This allows the OPC to provide ideas on best practices and offer early alerts about the privacy risks related to new programs and initiatives.

A key branch priority in 2007-2008 was to reduce a PIA review backlog. Over the year, the backlog of files waiting for review was significantly reduced from 50 files to 18.

We reviewed 78 PIAs for a wide range of government programs and initiatives. Some of these were for controversial and high-profile projects, such as Transport Canada's no-fly list and Canada Border Service Agency's Enhanced Driver's Licence initiative. Our Office also reviewed the privacy risks of lesser-known initiatives: a new benefits program for veterans; the recording of phone calls at Canada's ports; and the process for handling passport applications at Service Canada locations.

In most cases, we uncover privacy risks and make recommendations. Our advice is usually taken seriously.

Examples of Privacy Impact Assessment Reviews

Transport Canada – Passenger Protect Program (No-fly List)

While our Office continues to have significant concerns about the inherent privacy risks stemming from the no-fly list, our review of Transport Canada's PIA of the program did result in some improvements.

For example, in response to the OPC's recommendations, Transport Canada put in place our suggestions for passenger recourse; an audit of the program's effectiveness; confidentiality provisions in memoranda of understanding; and standard operating procedures for RCMP and CSIS to guide their actions when someone is denied boarding.

However, a recommendation that the personal information of individuals who are denied boarding not be shared with local police forces was not fully implemented.

Similarly, our proposal that the Passenger Protect Program, as well as other watch lists, be referred to a Parliamentary committee for review in an open and transparent forum was rejected.

Statistics Canada - Canada Health Measures Survey

Our review of the Canada Health Measures Survey – a national survey that will collect information from Canadians about their general health and lifestyles – initially recommended against the planned storage of survey participants' samples of blood, urine and DNA for unlimited lengths of time, to be used for unspecified future research.

Our Office felt this practice would render participants' consent to the collection of their samples somewhat meaningless.

The OPC recommended Statistics Canada store the biological samples, identified only by anonymous code, for a specific period of time, not exceeding 20 years. We also recommended the survey should not include the option of long-term storage for biological specimens from young respondents (aged 6 to 13 years) where consent was to be provided by a parent or guardian.

Statistics Canada decided to go ahead with the indefinite storage plan. It proposed that an oversight committee of interested parties such as the OPC could review the ways in which stored specimens may be used in the future. The plan to store children's biological samples will also proceed; however, those individuals will be contacted after their 14th birthdays to obtain explicit consent.

RCMP / Public Safety Canada – National Integrated Information Initiative

The National Integrated Information Initiative (N-III) is an electronic records-sharing program linking national, provincial and municipal police forces, with the capacity to expand access and sharing capabilities to federal government departments.

The initiative is a partnership involving the RCMP, Public Safety Canada and a number of departments and agencies such as the Canada Border Services Agency, Citizenship and Immigration Canada, the Canadian Firearms Centre, Correctional Service of Canada and the National Parole Board.

Given the significant number of institutions involved, the OPC asked Public Safety Canada to develop an over-arching PIA which would include a privacy management framework with measurable standards and limitations for all government agencies accessing and sharing information through systems, such as the Police Information Portal.

We had hoped such a PIA would: outline the overall business case defining and justifying the need for the proposed increased information sharing; articulate a Public Safety commitment to protect personal information; set measurable standards against which audits for compliance within each portfolio department could be accomplished; and include a communications strategy for informing Canadians about how the program may lead to their personal information being shared with a number of government institutions.

A year after the request was made, we have yet to receive an over-arching PIA, although our Office was informed in the spring of 2008 that work on a broad assessment had begun.

Canada Border Services Agency – Enhanced Drivers' Licences

Our Office has been working with the British Columbia Information and Privacy Commissioner during our review of the Enhanced Drivers' License (EDL) pilot project between British Columbia and Washington State. Canada Border Services Agency is encouraging and helping to coordinate the B.C. pilot as well as EDL projects in other provinces.

EDLs are being proposed as an alternative to a Canadian passport for travellers entering the United States at land borders. They are a response to new U.S. government rules requiring documentation of identity and citizenship.

Under the B.C. pilot, Canada Border Services Agency collects applicants' personal information from the province and transfers it to U.S. Customs and Border Protection.

Concerns raised during our PIA review include the duplication of personal information and data verification processes which already exist at Passport Canada. Other concerns include: unclear legislative authority for citizenship verification; meaningful consent; potential uses of personal information by the U.S. government; the use of EDLs for other purposes; and privacy risks related to the use of radio frequency identification (RFID) chips.

The OPC has pressed Canada Border Services Agency for assurances that subsequent EDL projects will not proceed on a permanent basis unless drivers' personal information remains in Canada, and that EDL information will only be used for crossing the border. While the way in which personal information will be disclosed to U.S. authorities was still under discussion as we prepared this report, Canada Border Services Agency has said the database itself will remain in Canada.

IN THE COURTS

As in previous years, there were only a few court applications proceeding under the *Privacy Act* in 2007-2008.

Under section 41 of the *Privacy Act*, the Federal Court may only review a government institution's refusal to grant access to personal information requested under the *Act*.

A section 41 application may *not* be made for wrongful collection, use or disclosure of an individual's personal information by a government institution.

Under section 41 of the *Privacy Act*, the Federal Court may only review a government institution's refusal to grant access to personal information requested under the *Act*.

Our Office has called on the federal government to broaden the grounds for which an application for court review under section 41 may be made to include the full array of privacy rights and protections under the *Privacy Act*. We also recommended giving the Federal Court the power to award damages against offending institutions.

Until the *Act* is amended, there will continue to be only a small number of court applications proceeding under the legislation.

The following cases of interest were before the Federal Court during 2007-2008.

In keeping with the spirit of our mandate, we do not publish the plaintiff's name in order to protect the privacy of the complainants. The court docket number and the name of the respondent institutions are listed.

X. v. Office of the Privacy Commissioner of Canada

Federal Court File T-1903-07

The Applicant filed a complaint against the Canadian Security Intelligence Service (CSIS) for failing to provide requested personal information. The Privacy Commissioner found the complaint was not well-founded.

The Applicant sought judicial review of the Privacy Commissioner's findings pursuant to section 41 of the *Act*. However, the purpose of a section 41 application is to ask the Court to determine whether the government institution against whom a complaint was filed respected the applicable provisions of the *Act* in refusing to provide access to personal information sought by the complainant. Section 41 does not provide for recourse against the Privacy Commissioner.

Mr. Justice Blanchard ruled that it is well established that the Privacy Commissioner has no decision-making authority and her findings and recommendations following an investigation under the *Act* are not binding on the government institution.

He also noted it is clear under the *Act* that it is not the Privacy Commissioner who is called upon to justify a refusal. That responsibility rests with the government institution refusing to grant access to requested personal information.

The Court therefore allowed the Privacy Commissioner's motion, ordering that the application proceed only on condition that the Applicant file an amended application directed at CSIS. The Applicant filed an amended application in March 2008.

Intervention in a Matter Involving the *Access to Information Act*

X. v. The Minister of Health Canada

Federal Court File No.: T-347-06

As reported in the 2006-2007 annual report, the Privacy Commissioner was granted intervener status in a case filed under the *Access to Information Act* which raises important privacy issues. Our Office was concerned about the possible re-identification of individuals when government information is combined with publicly available information.

The Applicant, a CBC producer, had sought access to Health Canada's Canadian Adverse Drug Reaction Information System – a database containing information relating to suspected adverse reactions to health products marketed in Canada.

In response to his request, Health Canada released some information, but refused to reveal the provinces in which data about adverse drug reactions had been collected on the grounds that it constituted personal information under the *Privacy Act*.

In a February 2008 decision, Mr. Justice Gibson accepted a fundamental premise set out by the Supreme Court of Canada: In a situation involving personal information about an individual, the right to privacy is paramount over the right of access to information.

He also adopted the legal test proposed by our Office: "Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."

Based on the evidence before him, Justice Gibson concluded that disclosure of the province would substantially increase the possibility that an individual could be identified based on the totality of data-fields already disclosed from the drug reaction

database, combined with other publicly available information, such as obituary notices. This is particularly the case for unique or quasi-unique individual reports, in smaller provinces or territories.

Therefore, in the circumstances, the province field does constitute personal information and was properly exempt from access.

Also of note, the judge emphasized the importance of ministerial discretion in deciding whether or not to exceptionally release this personal information in the public interest. In this case, the Minister had properly considered the facts before him and decided that, here, the public interest in disclosure did not clearly outweigh the violation of privacy that could result from the disclosure.

ACCESS TO INFORMATION AND PRIVACY UNIT

Our Office has now completed one full fiscal year subject to both the *Access to Information Act* and the *Privacy Act*. (The *Federal Accountability Act* extended both of these pieces of legislation so that they would cover our Office.)

We received 44 formal requests under the *Access to Information Act*. Fourteen of those requests were transferred to government institutions which had control of the records being sought, and we responded to 29 requests for access to information in our Office. One other request was carried over. All *Access to Information Act* requests were responded to within the statutory time frames.

Our Office received five complaints from two people under the *Access to Information Act* – three alleged denial of access and two concerned response time. The Information Commissioner concluded two access complaints were “not substantiated” and the third was “resolved.” The Information Commissioner further concluded that one time complaint was “not substantiated” and the other was “resolved.”

Our Office received 45 requests for personal information under the *Privacy Act*. We redirected 23 requests to government institutions which had the information being sought, and we responded to 22 requests for access to OPC information. All *Privacy Act* requests were responded to within the statutory time frames set out in the *Act*.

The OPC received two complaints under the *Privacy Act* from one individual alleging denial of access. The complaints were addressed under an arms-length process and were determined to be “not well-founded” in April 2008.

The *Federal Accountability Act* does not include a mechanism under which *Privacy Act* complaints against our Office would be investigated. Given the fact it would be entirely inappropriate for our Office to investigate its own actions with respect

to its administration of the *Privacy Act*, we have created the position of “Privacy Commissioner ad hoc” to conduct such investigations.

In September 2007, the Honourable Mr. Justice Peter Cory was engaged as Privacy Commissioner ad hoc. The Privacy Commissioner delegated to him the majority of her powers, duties and functions as set out in sections 29 through 35 and section 42 of the *Act*. Justice Cory completed his contract in March 2008. A new Privacy Commissioner ad hoc, Justice Andrew Mackay, has since assumed these duties.

A substantial number of the requests we have received under both the *Access to Information Act* and the *Privacy Act* were for the contents of our investigation files. In a few cases, all file information was withheld as required by the *Access to Information Act* and the *Privacy Act* because the investigation or court proceedings were ongoing. Where an investigation was fully concluded, the file information was processed and access was granted subject to relevant exemptions.

INTERNATIONAL CONFERENCE

As reported in our 2007 PIPEDA Annual Report, the success of the 29th International Conference of Data Protection and Privacy Commissioners – held in Montreal in September and following through on our initial 2002 engagement – was beyond our highest expectations.

We welcomed more than 600 commissioners, academics, privacy professionals, advocates, government officials, IT specialists and others from around the globe – making it the largest-ever conference of its kind. Most importantly, the positive reviews and kudos from participants justified the time and resources invested in this event.

The conference theme was Privacy Horizons: *Terra Incognita*. Early cartographers marked unknown lands that had yet to be mapped with this Latin term. One of the earliest known terrestrial globes from Europe labels an uncharted edge of the ocean “*hic sunt dracones*” – or “here be dragons.”

This notion of an unknown landscape with lurking dragons seemed the perfect metaphor for the future of privacy. Privacy issues are changing rapidly, with powerful new technologies and the international war on terror acting as potent forces which threaten the privacy of people around the world.

The goal of our conference was to begin to chart what the privacy world of the future might look like and also to equip privacy advocates with some strong dragon-slaying tools. During a series of plenaries, workshops and information sessions, we considered the best strategies for defending privacy rights in the face of constant change.

Participants heard from the who's who of the privacy world, including security technology guru and author Bruce Schneier; Simon Davies, a pioneer of the international privacy arena and founder of Privacy International; consumer privacy advocate Katherine Albrecht; Marc Rotenberg, executive director of the Electronic Privacy Information Center; Peter Fleischer, Google's global privacy counsel; Peter Hustinx, the European Data Protection Supervisor; as well as Peter Schaar, now past-chair of the EU Article 29 Data Protection Working Party and France's Alex Türk, who is now chair of the working party. Our guest of honour, who opened the conference, was the Honourable Peter Milliken, Speaker of the House of Commons.

The conference program underscored the wide range of issues which will have an impact on privacy in the coming years as well as the increasingly global nature of privacy issues.

We prepared 14 workbooks before the conference. Most included a commissioned paper by a subject-matter expert and a variety of other resources, such as research and bibliographical materials, to satisfy the curiosity of participants who might be new to a particular subject, as well as the more rigorous requirements of key policy and decision-makers to locate trustworthy information about the privacy implications of our conference topics. These are available on our conference website at www.privacyconference2007.gc.ca and are an important legacy of the conference.

We have posted details about the cost of the conference on our website. We stayed well within our overall financial targets.

THE YEAR AHEAD

The list of issues our Office deals with on a daily basis will always be a lengthy one. In an effort to focus our efforts on the most significant threats to the privacy of Canadians, we have identified four top strategic priorities: information technology, national security, identity integrity and protection, and genetic information.

A key objective for our Office over 2008-2009 will be to **provide leadership on our priority issues**. Our plans to address these privacy threats include the following steps:

- **Information Technology**
 - Build sufficient capacity to assess the privacy impact of new information technologies.
 - Increase public awareness of technologies with potential privacy impacts.
 - Provide practical guidance to organizations on the implementation of specific technologies.
- **National Security**
 - Ensure national security initiatives adequately protect privacy.
 - Ensure proper oversight and accountability of national security agencies' personal information management practices.
 - Raise public awareness of the privacy impacts of national security initiatives.
- **Identity Integrity and Protection / Identity Theft**
 - Improve organizations' personal information management practices.
 - Raise public awareness of identity protection.
 - Advocate for a coordinated federal government approach to identity protection.

- **Genetic Information**

- Advance research and knowledge to address new challenges posed by genetics in the context of traditional data protection regimes.
- Raise public awareness about the potential uses of genetic information.

Our Office has identified four other major corporate priorities. They are:

- Continue to **improve service delivery** through focus and innovation, including new investigative strategies to make our complaints resolution process more efficient;
- **Build a sustainable organizational capacity** by growing our Office and continuing an information management renewal project;
- **Support Canadians** to make informed privacy decisions with expanded public education initiatives such as a social marketing campaign on children's online privacy and outreach programs in partnership with provincial and territorial privacy commissioners; and
- Strategically **advance global privacy protection for Canadians** through work with organizations such as the OECD and APEC.

APPENDIX 1

DEFINITIONS OF COMPLAINT TYPES

Complaints received in the OPC are categorized into three main groups:

Access:

- **Access** – All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.
- **Correction/Notation** – The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.
- **Language** – Personal information was not provided in the official language of choice.
- **Fee** – Fees have been assessed to respond to a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.
- **Index** – Infosource (a federal government directory that describes each institution and the banks of information – groups of files on the same subject – held by that particular institution) does not adequately describe the personal information holdings of an institution.

Privacy:

- **Collection** – Personal information collected is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.
- **Retention and Disposal** – Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in Infosource): either destroyed too soon or kept too long.

In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.

- **Use and Disclosure** – Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible uses or disclosures without consent set out in sections 7 and 8 of the *Act*.

Time Limits:

- **Time Limits** – The institution did not respond within the statutory limits.
- **Extension Notice** – The institution did not provide an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.
- **Correction/Notation - Time Limits** – The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

DEFINITIONS OF FINDINGS AND OTHER DISPOSITIONS UNDER THE *PRIVACY ACT*

The OPC has developed a series of definitions of findings to explain the outcome of its investigations under the *Privacy Act*.

Early resolution: Applied to situations in which the issue is dealt with before a formal investigation is undertaken. For example, if an individual complains about an issue the OPC has already investigated and found to be compliant with the *Privacy Act*, we explain this to the individual. We also receive complaints in which a formal investigation could have adverse implications for the individual. We discuss the possible impact at length with the individual and should he or she choose not to proceed further, the file is closed as “early resolution”.

Not Well-founded: The investigation uncovered no or insufficient evidence to conclude that the government institution violated the complainant’s rights under the *Privacy Act*.

Well-founded: The government institution failed to respect the *Privacy Act* rights of an individual.

Well-founded/Resolved: The investigation substantiated the allegations and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: After a thorough investigation, the OPC helped negotiate a solution that satisfied all parties. The finding is used for those complaints in which well-founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

Settled during the course of the investigation: The OPC helped negotiate a solution that satisfied all parties during the investigation, but did not issue a finding.

Discontinued: The investigation was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons —the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

APPENDIX 2

INVESTIGATION PROCESS UNDER THE *PRIVACY ACT*

Inquiry:

Individual contacts OPC by letter, by telephone, or in person to complain of violation of the Act. Individuals who make contact in person or by telephone must subsequently submit their allegations in writing.



Initial analysis:

Inquiries staff review the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act.

An individual may complain about any matter specified in section 29 of the *Privacy Act* – for example, denial of access, or unacceptable delay in providing access to his or her personal information held by an institution; improper collection, use or disclosure of personal information; or inaccuracies in personal information used or disclosed by an institution.



Complaint?

No:

The individual is advised, for example, that the matter is not in our jurisdiction.

Yes:

An investigator is assigned to the case.

Early resolution?

A complaint may be resolved before an investigation is undertaken if, for example, the issue has already been fully dealt with in another complaint and the institution has ceased the practice or the practice does not contravene the Act.

Investigation:

The investigation provides the factual basis for the Commissioner to determine whether the individual's rights under the *Privacy Act* have been contravened.

The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner or her delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

Discontinued?

A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.

Analysis (on next page)

Settled? (on next page)

Note: a broken line (---) indicates a *possible* outcome.

Analysis:

The investigator analyzes the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Branches, as appropriate.

Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the institution are warranted.

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the institution. The Privacy Commissioner or her delegate may ask the institution to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.

The possible findings are:

Not Well-Founded: The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the *Act* have been contravened.

Well-Founded: The institution failed to respect a provision of the *Act*.

Well-Founded, Resolved: The investigation substantiated the allegations and the institution has agreed to take corrective measures to rectify the problem.

Resolved: The evidence gathered in the investigation supports the allegations raised in the complaint, but the institution agreed to take corrective measures to rectify the problem, to the satisfaction of this Office. The finding is used for those complaints in which Well-Founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court on matters of denial of access to personal information.

Where recommendations have been made to an institution, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the denial of access. The Federal Court has the power to review the matter and determine whether the institution must provide the information to the requester.

Note: a broken line (---) indicates a *possible* outcome.

APPENDIX 3

PRIVACY ACT INQUIRY, COMPLAINT AND INVESTIGATION STATISTICS FOR 2007-2008

Inquiries

Our Inquiries Unit received well over 4,000 *Privacy Act*-related inquiries between April 1, 2007 and March 31, 2008.

Some of the most frequently raised issues included ways in which to make formal requests for access to personal information; how to file complaints against government institutions that, for example, exceed statutory time limits and fail to comply with the *Privacy Act*. We also received inquiries from individuals seeking advice from our Office as a result of being affected by various privacy breaches.

Privacy Act inquiries received by the Inquiries Unit

Telephone inquiries	2,199
Written inquiries (letter, e-mail, fax)	2,059
Total number of inquiries received	4,258

Privacy Act inquiries closed

Telephone inquiries	2,221
Written inquiries (letter, e-mail, fax)	1,901
Total number of inquiries closed	4,122

General inquiries received *

Telephone inquiries	2,231
Written inquiries (letter, e-mail, fax)	136
Total number of inquiries received	2,367

General inquiries closed

Telephone inquiries	2,229
Written inquiries (letter, e-mail, fax)	140
Total number of inquiries closed	2,369

*These are inquiries related to privacy issues, but cannot be linked to either Act.

Complaints Received by Type

Complaint Type	Count	Percentage
Access	292	38
Time Limits	259	34
Use and Disclosure	124	16
Collection	33	4
Correction-Time Limits	26	3
Extension Notice	10	1
Retention and Disposal	9	1
Correction-Notation	5	1
Language	1	< 1
Total	759	

As in previous years, the most common complaints to our Office related to both access to personal information as well as the length of time government departments and agencies take to respond to access requests.

See Appendix 1 for definitions of complaint types.

Top Ten Institutions by Complaints Received

	Total	Access to Personal Information	Time Limits	Privacy
Correctional Service Canada	248	48	151	49
Royal Canadian Mounted Police	84	59	14	11
Canada Border Services Agency	54	18	31	5
Service Canada	52	13	14	25
National Defence	48	17	19	12
Canadian Security Intelligence Service	45	44	0	1
Canada Revenue Agency	38	18	9	11
Canada Post Corporation	28	16	8	4
Foreign Affairs and International Trade	27	6	7	14
Justice Canada	18	4	13	1
Others	117	49	29	39
Total	759	292	295	172

Some institutions – because of their mandate – hold a substantial amount of personal information and are more likely to receive numerous requests for access to that information and subsequent complaints.

See Appendix 1 for definitions of complaint types.

Complaints Received by Institution

	Total
Correctional Service Canada	248
Royal Canadian Mounted Police	84
Canada Border Services Agency	54
Service Canada	52
National Defence	48
Canadian Security Intelligence Service	45
Canada Revenue Agency	38
Canada Post Corporation	28
Foreign Affairs and International Trade Canada	27
Justice Canada	18
Human Resources and Social Development Canada	14
Citizenship and Immigration Canada	14
Health Canada	8
Transport Canada	7
Public Works and Government Services Canada	6
Fisheries and Oceans	5
Library and Archives Canada	5
Privy Council Office	5
Agriculture and Agri-Food Canada	4
Canadian Food Inspection Agency	4
Indian and Northern Affairs Canada	4
Treasury Board of Canada Secretariat	4
Commission for Public Complaints Against the RCMP	3
Environment Canada	3
Public Service Commission Canada	3
Canada Firearms Centre	2
Canada Mortgage and Housing Corporation	2
Canada Public Service Agency	2
Ombudsman National Defence and Canadian Forces	2
Canadian Broadcasting Corporation	1
Canadian Forces Grievance Board	1
Canadian Human Rights Agency	1
Canadian Transportation Agency	1
Correctional Investigator Canada	1
Export Development Corporation	1
Financial Transactions and Reports Analysis Centre of Canada	1
Immigration and Refugee Board	1
Industry Canada	1
Inspector General of the Canadian Security Intelligence Service, Office of the	1
National Museum of Science and Technology	1
National Parole Board	1
Natural Resources Canada	1
Pension Appeals Board Canada	1
Public Safety Canada	1
Public Service Labour Relations Board	1
Public Service Staffing Tribunal	1
Royal Canadian Mint	1
Statistics Canada	1
Veteran Affairs Canada	1
Total	759

Complaints Received by Province/Territory

	Total	Percentage
Ontario	195	26
British Columbia	179	23
NCR	112	15
Quebec	65	8
Alberta	60	8
Saskatchewan	44	6
Nova Scotia	28	4
Manitoba	26	3
International *	22	3
New Brunswick	15	2
Newfoundland	5	1
Prince Edward Island	4	1
Nunavut	3	<1
Yukon Territory	1	<1
Total	759	

* Canadians living abroad have the same access and privacy protection rights under the *Privacy Act* as those living in Canada, including the right to complain to this Office. Some of these Canadians living abroad have chosen to exercise those rights. (Note: the privacy protection rights, but not access rights, are also available to all individuals of any citizenship or country of residence.)

We have seen one significant change in the geographical distribution of complaints over the last few years: There has been a sharp drop in the number of Quebec complaints, which accounted for 24 per cent of total complaints in 2005-2006; 14 per cent in 2006-2007; and just 8 per cent in 2007-2008. While we can't be certain about the precise reason for this decrease, we are aware that Quebec has its own stringent privacy legislation. Most of our complainants living in Quebec who use our services, are located in the National Capital Region.

Closed Complaints by Finding

Finding	Count	Percentage
Early Resolution	32	4
Settled	114	13
Well-founded Resolved	17	2
Resolved	6	< 1
Well-founded	319	36
Not Well-founded	275	31
Discontinued	117	13
Total	880	

Roughly one in five of our closed complaints resulted in solutions that satisfied complainants, respondents and our Office – with an Early Resolution, Settled, Well-founded Resolved or Resolved finding. A significant number of closed complaints – more than one third – were well founded, which suggests that there is room for improvement in privacy management practices.

Findings by Complaint Type

Complaints (All Types) Closed

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded/Resolved	Total
Access	56	4	180	5	59	2	12	318
Time Limits	14	18	23	0	3	243	0	301
Use and Disclosure	32	4	51	1	31	42	3	164
Collection	6	5	11	0	11	0	0	33
Correction-Time Limits	3	1	0	0	5	22	0	31
Extension Notice	1	0	3	0	0	10	0	14
Retention and Disposal	3	0	4	0	4	0	1	12
Correction-Notation	2	0	3	0	1	0	1	7
Total	117	32	275	6	114	319	17	880

This table shows varying characteristics by Complaint Type. For instance, by their very nature, most Time Limits are well-founded; most individuals do not complain to us until the statutory deadline has passed. Seventy-five per cent of Access cases are either not well-founded or settled, meaning that the exemptions were properly claimed and/or individuals were satisfied with the explanation given of the reasons for exemptions or missing documentation. Interestingly, no Collection complaints were well-founded. This indicates several possible things: that the collection of personal information was indeed necessary and reasonable for the program or activity of the government institution;

that the individuals understood an explanation/rationale for the collection; or that discussions with the organizations were successful in reaching some compromise that was acceptable to both parties.

Access and Privacy Complaints Closed

	Discontinued	Early Resolution	Settled in course of investigation	Not well-founded	Well-founded	Well-founded-Resolved	Resolved	Total
Access	56	4	59	180	2	12	5	318
Use and Disclosure	32	4	31	51	42	3	1	164
Collection	6	5	11	11	0	0	0	33
Retention and Disposal	3	0	4	4	0	1	0	12
Correction-Notation	2	0	1	3	0	1	0	7
Total	99	13	106	249	44	17	6	534

As in previous years, not well-founded complaints outweigh those complaints that are well-founded. In addition, a number of complaints have been concluded using alternate resolution mechanisms, as is demonstrated by the number of settled complaints and early resolution findings.

See Appendix 1 for definitions of findings and other dispositions under the *Privacy Act*.

Time Limits Complaints Closed

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded/Resolved	Total
Time Limits	14	18	23	0	3	243	0	301
Correction-Time Limits	3	1	0	0	5	22	0	31
Extension Notice	1	0	3	0	0	10	0	14
Total	18	19	26	0	8	275	0	346

By their very nature, the majority of time limits complaints are well-founded. The requirements for federal departments and agencies are clear: They have 30 days to respond to requests for access to personal information. Some time limits complaints are not well-founded because the organization has appropriately applied an extension notice, which allows for an additional 30 days to respond.

Time Limits Complaints Closed by Institution and Finding

As indicated in the following table, Correctional Services Canada has, by far, the highest number of Time Limits complaints. This is a reflection of the large volume of personal information it holds on inmates and the large number of requests it receives from that population. That institution recently received a significant increase in resources to address the volume. Likewise, National Defence, Canada Border Services Agency, the RCMP and the Canada Revenue Agency all have significant holdings of personal information and therefore face significant challenges in responding in a timely fashion to the high volume of requests they receive, with the resources they have available.

	Discontinued	Early Resolution	Not well-founded	Settled in course of investigation	Well-founded	Total
Correctional Service Canada	5	14	3	6	146	174
National Defence	2	0	0	0	26	28
Canada Border Services Agency	1	0	1	0	25	27
Royal Canadian Mounted Police	4	1	1	0	15	21
Canada Revenue Agency	0	0	3	1	14	18
Justice Canada	0	0	0	0	13	13
Service Canada	3	0	1	0	6	10
Canadian Security Intelligence Service	0	0	8	0	0	8
Foreign Affairs and International Trade Canada	0	0	0	0	8	8
Canada Post Corporation	0	2	0	0	3	5
Citizenship and Immigration Canada	0	0	0	0	5	5
Human Resources and Social Development Canada	1	0	2	0	2	5
Canada Firearms Centre	0	0	3	0	0	3
Privy Council Office	1	0	0	0	2	3
Public Works and Government Services Canada	0	0	0	0	3	3
Agriculture and Agri-Food Canada	0	0	2	0	0	2
Health Canada	0	0	0	0	2	2
Indian and Northern Affairs Canada	0	0	0	0	2	2
Library and Archives Canada	1	1	0	0	0	2
Correctional Investigator Canada, Office of the	0	1	0	0	0	1
Environment Canada	0	0	0	0	1	1
Export Development Corporation	0	0	0	0	1	1
Fisheries and Oceans	0	0	0	0	1	1
Inspector General of the Canadian Security Intelligence Service, Office of the	0	0	1	0	0	1
Public Safety Canada	0	0	0	1	0	1
Treasury Board of Canada Secretariat	0	0	1	0	0	1
Total	18	19	26	8	275	346

The increase in the number of well-founded time limit complaints can be directly attributed to the increase in requests institutions receive and the limited resources available to them. This trend affects the majority of government institutions.

Access and Privacy Complaints Closed by Institution and Finding

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded/Resolved	Total
Correctional Service Canada	26	1	39	2	21	21	4	114
Canada Revenue Agency	9	1	41	0	11	6	1	69
Immigration and Refugee Board	0	0	58	0	0	0	0	58
Royal Canadian Mounted Police	11	2	24	1	9	3	2	52
Citizenship and Immigration Canada	7	1	16	0	11	0	0	35
National Defence	10	1	9	0	3	2	1	26
Canada Post Corporation	8	1	4	1	10	0	0	24
Human Resources and Social Development Canada	11	1	5	0	2	1	2	22
Service Canada	3	1	7	1	7	2	1	22
Canada Border Services Agency	2	0	5	1	4	2	1	15
Foreign Affairs and International Trade Canada	1	1	6	0	2	4	0	14
Justice Canada, Department of	2	0	4	0	2	1	1	10
Fisheries and Oceans	0	0	0	0	7	0	0	7
National Parole Board	1	0	1	0	2	0	2	6
Canadian Security Intelligence Service	0	0	5	0	0	0	0	5
Health Canada	0	1	2	0	2	0	0	5
Indian and Northern Affairs Canada	1	0	1	0	3	0	0	5
Environment Canada	0	0	4	0	0	0	0	4
Library and Archives Canada	2	0	0	0	2	0	0	4
Statistics Canada	1	1	1	0	1	0	0	4
Transport Canada	2	0	2	0	0	0	0	4
Canadian Human Rights Commission	1	0	1	0	0	0	1	3
Freshwater Fish Marketing Corporation	0	0	0	0	3	0	0	3
Public Service Commission Canada	0	0	2	0	1	0	0	3
Canada School for Public Service	0	0	2	0	0	0	0	2
Privy Council Office	0	0	1	0	0	1	0	2
Public Safety Canada	0	0	0	0	2	0	0	2

Access and Privacy Complaints Closed by Institution and Finding (cont.)

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded/Resolved	Total
Public Works and Government Services Canada	0	0	0	0	1	1	0	2
Treasury Board of Canada Secretariat	0	0	2	0	0	0	0	2
Agriculture and Agri-Food Canada	0	0	1	0	0	0	0	1
Canadian Air Transport Security Authority	0	0	1	0	0	0	0	1
Canadian Food Inspection Agency	0	0	1	0	0	0	0	1
Canadian Space Agency	0	0	1	0	0	0	0	1
Canadian Transportation Agency	1	0	0	0	0	0	0	1
Export Development Corporation	0	0	0	0	0	0	1	1
Industry Canada	0	1	0	0	0	0	0	1
Inspector General of the Canadian Security Intelligence Service, Office of the	0	0	1	0	0	0	0	1
Office of the Chief Electoral Officer	0	0	1	0	0	0	0	1
Veterans Affairs Canada	0	0	1	0	0	0	0	1
Total	99	13	249	6	106	44	17	534

Complaint Investigations Treatment Times - *Privacy Act*

Treatment times are the average number of months to complete a complaint investigation, from the date the complaint is received to when a finding is made.

By Finding

Disposition	Average Treatment Time in Months
Early Resolution	6.25
Well-founded	6.32
Resolved	16.17
Discontinued	16.57
Settled in the Course of Investigation	17.87
Not Well-founded	21.67
Well-founded Resolved	27.24
Overall Average	14.45

The significant difference between treatment times for well-founded complaints and not well-founded complaints arises from Time Limits complaints. They represent 34 per cent of our caseload, the majority of which are well-founded, and the majority of which are closed relatively quickly compared to other types of complaints.

By Complaint Type

Complaint Type	Average Treatment Time in Months
Time Limits	4.58
Extension Notice	6.07
Correction/Time Limit	7.10
Correction/Notation	13.14 *
Collection	16.09
Use and Disclosure	18.68
Access	22.14
Overall Average	14.40

* The treatment time for this complaint type reflects seven cases.

Durée de traitement des enquêtes faisant suite à des plaintes – Loi sur la protection des renseignements personnels

La durée de traitement est la durée moyenne (en mois) d'une enquête faisant suite à une plainte, à compter de la date de réception de la plainte jusqu'à la date à laquelle une conclusion est formulée.

Par conclusion

Conclusion	Durée de traitement moyen (en mois)
Réglée rapidement	6,25
Fondée	6,32
Résolue	16,17
Abandonnée	16,57
Réglée en cours d'enquête	17,87
Non fondée	21,67
Fondée et résolue	27,24
Moyenne générale	14,45

L'écart important entre la durée de traitement des plaintes fondées et celle des plaintes non fondées provient des plaintes liées aux délais. Ces plaintes représentent 34 p. 100 des dossiers traités et la majorité d'entre elles sont fondées et sont fermées relativement rapidement en comparaison des autres types de plaintes.

Par type de plainte

Type de plainte	Durée de traitement moyen (en mois)
Délais	4,58
Avis de prorogation	6,07
Correction/délais	7,10
Correction/annotation	13,14*
Collecte	16,09
Utilisation et communication	18,68
Accès	22,14
Moyenne générale	14,40

* Le délai de traitement pour ce genre de plainte se fonde sur sept cas.

Plaintes fermées par institution et par conclusions – accès et protection des renseignements personnels (suite)

Institution	Révisé	Régler rapidement	Non fondé	Régler en cours	Fondé	Fondé et résolu	Total
-------------	--------	-------------------	-----------	-----------------	-------	-----------------	-------

Travaux publics et Services gouvernementaux Canada	0	0	0	1	1	0	2
Secrétariat du Conseil du Trésor du Canada	0	0	2	0	0	0	2
Agriculture et Agroalimentaire Canada	0	0	1	0	0	0	1
Administration canadienne de la sûreté du transport aérien	0	0	1	0	0	0	1
Agence canadienne d'inspection des aliments	0	0	1	0	0	0	1
Agence spatiale canadienne	0	0	1	0	0	0	1
Office des transports du Canada	1	0	0	0	0	0	1
Exportation et développement Canada	0	0	0	0	0	1	1
Industrie Canada	0	1	0	0	0	0	1
Bureau de l'inspecteur général du Service canadien du renseignement de sécurité	0	0	1	0	0	0	1
Bureau du directeur général des élections	0	0	1	0	0	0	1
Anciens Combattants Canada	0	0	1	0	0	0	1
Total	99	13	249	6	106	44	534

Plaintes fermées par institution et par conclusions – accès et protection des renseignements personnels

Intitulé	Abandonnée	Réglée rapidement	Non fondée	Réglée	Réglée en cours	Réglée	Fondée	Fondée et résolue	Total
----------	------------	-------------------	------------	--------	-----------------	--------	--------	-------------------	-------

Service correctionnel du Canada	26	1	39	2	21	21	4	114	
Agence du revenu du Canada	9	1	41	0	11	6	1	69	
Commission de l'immigration et du statut de réfugié	0	0	58	0	0	0	0	58	
Gendarmerie royale du Canada	11	2	24	1	9	3	2	52	
Citoyenneté et Immigration Canada	7	1	16	0	11	0	0	35	
Défense nationale	10	1	9	0	3	2	1	26	
Société canadienne des postes	8	1	4	1	10	0	0	24	
Ressources humaines et Développement social Canada	11	1	5	0	2	1	2	22	
Service Canada	3	1	7	1	7	2	1	22	
Agence des services frontaliers du Canada	2	0	5	1	4	2	1	15	
Affaires étrangères et Commerce international Canada	1	1	6	0	2	4	0	14	
Justice Canada	2	0	4	0	2	1	1	10	
Pêches et Océans Canada	0	0	0	0	7	0	0	7	
Commission nationale des libérations conditionnelles	1	0	1	0	2	0	2	6	
Service canadien du renseignement de sécurité	0	0	5	0	0	0	0	5	
Santé Canada	0	1	2	0	2	0	0	5	
Affaires indiennes et du Nord Canada	1	0	1	0	3	0	0	5	
Environnement Canada	0	0	4	0	0	0	0	4	
Bibliothèque et Archives Canada	2	0	0	0	2	0	0	4	
Statistique Canada	1	1	1	0	1	0	0	4	
Transports Canada	2	0	2	0	0	0	0	4	
Commission canadienne des droits de la personne	1	0	1	0	0	0	1	3	
Office de commercialisation du poisson d'eau douce	0	0	0	0	3	0	0	3	
Commission de la fonction publique du Canada	0	0	2	0	1	0	0	3	
École de la fonction publique du Canada	0	0	2	0	0	0	0	2	
Bureau du Conseil privé	0	0	1	0	0	1	0	2	
Sécurité publique Canada	0	0	0	0	2	0	0	2	

Plaintes liées aux délais fermées par institution fédérale et par conclusions d'enquête

Tel qu'indiqué dans le tableau suivant, le Service correctionnel du Canada a, de loin, le plus grand nombre de plaintes liées aux délais en raison du grand volume de renseignements personnels qu'il détient au sujet des détenus et du grand nombre de demandes qu'il reçoit de la population carcérale. L'institution a récemment augmenté considérablement ses ressources afin de traiter ces demandes. De même, la Défense nationale, l'Agence des services frontaliers du Canada, la GRC et l'Agence du revenu du Canada possèdent d'importants fonds de renseignements personnels et font donc face à d'importants défis si elles souhaitent répondre en temps opportun au grand nombre de demandes qu'elles reçoivent au moyen des ressources en place.

	Abandonnée	Réglée rapidement	Non fondée	Réglée en cours d'enquête	Fondée	Total
Service correctionnel du Canada	5	14	3	6	146	174
Défense nationale	2	0	0	0	26	28
Agence des services frontaliers du Canada	1	0	1	0	25	27
Gendarmerie royale du Canada	4	1	1	0	15	21
Agence du revenu du Canada	0	0	3	1	14	18
Justice Canada	0	0	0	0	13	13
Service Canada	3	0	1	0	6	10
Service canadien du renseignement de sécurité	0	0	0	0	0	8
Affaires étrangères et Commerce international Canada	0	0	8	0	0	8
Société canadienne des postes	0	2	0	0	0	8
Citoyenneté et Immigration Canada	0	0	0	0	5	5
Ressources humaines et Développement social Canada	1	0	2	0	2	5
Centre des armes à feu Canada	0	0	0	0	0	3
Bureau du Conseil privé	1	0	0	0	2	3
Travaux publics et Services gouvernementaux Canada	0	0	0	0	3	3
Agriculture et Agroalimentaire Canada	0	0	2	0	0	2
Santé Canada	0	0	0	0	2	2
Affaires indiennes et du Nord Canada	0	0	0	0	2	2
Bibliothèque et Archives Canada	1	1	0	0	0	2
Bureau de l'Enquêteur correctionnel du Canada	0	1	0	0	0	1
Environnement Canada	0	0	0	0	0	1
Exportation et développement Canada	0	0	0	0	1	1
Pêches et Océans Canada	0	0	0	0	1	1
Bureau de l'inspecteur général du Service canadien du	0	0	1	0	0	1
renseignement de sécurité	0	0	0	0	0	1
Sécurité publique Canada	0	0	0	1	0	1
Secrétariat du Conseil du Trésor du Canada	0	0	1	0	0	1
Total	18	19	26	8	275	346

L'augmentation du nombre de plaintes liées aux délais qui sont fondées peut être directement attribuable à la hausse de demandes que reçoivent les institutions et aux ressources limitées dont celles-ci disposent. Cette tendance touche la plupart des institutions fédérales.

était nécessaire et raisonnable aux fins des programmes ou des activités de l'institution gouvernementale; les personnes ont compris les explications ou les motifs invoqués pour la collecte; les discussions avec l'organisation ont permis d'en arriver à un compromis acceptable pour les deux parties.

Plaintes fermées – accès et protection des renseignements personnels

	Accès	Abandonnée	Réglée rapidement	Non fondée	Résolue	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
Utilisation et communication	32	4	51	1	31	42	3	164	318
Collecte	6	5	11	0	11	0	0	33	33
Conservation et retrait	3	0	4	0	4	0	1	12	12
Correction/annotation	2	0	3	0	0	1	0	7	7
Total	99	13	249	6	106	44	17	534	534

Comme au cours des exercices précédents, le nombre de plaintes non fondées dépasse celui des plaintes fondées. En outre, plusieurs plaintes ont été réglées au moyen d'autres mécanismes de résolution, comme le démontre le nombre de plaintes réglées en cours d'enquête et réglées rapidement.

Vous trouverez des définitions des conclusions et d'autres dispositions en vertu de la Loi sur la protection des renseignements personnels à l'annexe 1.

Plaintes fermées – délais

	Abandonnée	Réglée rapidement	Non fondée	Résolue	Réglée en cours d'enquête	Fondée	Fondée et résolue	Total
Délais	14	18	23	0	3	243	0	301
Correction/délais	3	1	0	0	5	22	0	31
Avis de prorogation	1	0	3	0	0	10	0	14
Total	18	19	26	0	8	275	0	346

De par leur nature, la plupart des plaintes liées aux délais sont fondées. Les exigences imposées aux ministères et aux organismes gouvernementaux sont claires : les institutions disposent de 30 jours pour fournir aux personnes qui en font la demande l'accès à leurs renseignements personnels. Certaines plaintes sur les délais ne sont pas fondées parce que des avis de prorogation ont été appliqués de manière légitime. Ces prorogations accordent un délai additionnel de 30 jours pour répondre à une demande.

Plaintes fermées par conclusion

Conclusion		Conclunion	
Réglée rapidement	Réglée	Fondée et résolue	Réglée
32	114	17	2
4	13	2	6
Pourcentage		Nombre	
		880	

Près d'une plainte fermée sur cinq s'est soldée par une solution qui satisfaisait les plaignants, les intimés et le Commissariat (plainte réglée rapidement, réglée, fondée et résolue ou résolue). Un nombre important de plaintes fermées, soit plus du tiers, étaient fondées, ce qui donne à penser qu'il y a matière à amélioration en ce qui concerne les pratiques de gestion de la protection de la vie privée.

Conclusions par type de plainte

Plaintes fermées (tous les types)

Abandonnée	Réglée rapidement	Non fondée	Réglée	en cours d'enquête	Fondée	Fondée et résolue	Total
56	4	180	5	59	2	12	318
14	18	23	0	3	243	0	301
32	4	51	1	31	42	3	164
6	5	11	0	11	0	0	33
3	1	0	0	5	22	0	31
1	0	3	0	0	10	0	14
3	0	4	0	4	0	1	12
2	0	3	0	1	0	1	7
117	32	275	6	114	319	17	880
Total							
Correction/annotation	2	0	0	1	0	1	7
retrait							
Conservation et prorogation	3	0	0	4	0	1	12
Avis de	1	0	0	0	10	0	14
Correction/ délais	3	1	0	5	22	0	31
Collecte	6	5	11	0	0	0	33
Utilisation et communication	32	4	51	1	42	3	164
Délais	14	18	23	0	243	0	301
Accès	56	4	180	5	59	2	318

Plaintes reçues par province/territoire

Pourcentage	Total	
26	195	Ontario
23	179	Colombie-Britannique
15	112	Région de la capitale nationale
8	65	Québec
8	60	Alberta
6	44	Saskatchewan
4	28	Nouvelle-Écosse
3	26	Manitoba
3	22	International*
2	15	Nouveau-Brunswick
1	5	Terre-Neuve-et-Labrador
1	4	Île-du-Prince-Édouard
<1	3	Nunavut
<1	1	Yukon
	759	Total

* Les Canadiennes et les Canadiens vivant à l'étranger ont les mêmes droits d'accès et de protection des renseignements personnels conférés par la *Loi sur la protection des renseignements personnels* que les Canadiennes et les Canadiens vivant au Canada; notamment le droit de déposer une plainte au Commissariat. Certains d'entre eux ont choisi d'exercer ces droits. (Note : Le droit à la protection des renseignements personnels, contrairement au droit d'accès, est aussi accordé à tous les individus, peu importe leur citoyenneté ou leur pays de résidence.)

Nous avons constaté un changement important en ce qui concerne la provenance des plaintes au cours des dernières années : il y a eu une nette diminution dans le nombre de plaintes provenant du Québec, qui comptaient pour 24 p. 100 du nombre total de plaintes en 2005-2006; 14 p. 100 en 2006-2007 et seulement 8 p. 100 en 2007-2008. Bien que nous ne puissions déterminer avec certitude la raison précise de cette diminution, nous sommes conscients que le Québec est doté de lois strictes en matière de protection de la vie privée. La plupart des plaignants vivant au Québec qui ont recours à nos services habitent dans la région de la capitale nationale.

Plaintes reçues par institution gouvernementale

248	Service correctionnel du Canada
84	Gendarmerie royale du Canada
54	Agence des services frontaliers du Canada
52	Service Canada
48	Défense nationale
45	Service canadien du renseignement de sécurité
38	Agence du revenu du Canada
28	Société canadienne des postes
27	Affaires étrangères et Commerce international Canada
18	Justice Canada
14	Ressources humaines et Développement social Canada
14	Citoyenneté et Immigration Canada
8	Santé Canada
7	Transports Canada
6	Travaux publics et Services gouvernementaux Canada
5	Pêches et Océans Canada
5	Bibliothèque et Archives Canada
5	Bureau du Conseil privé
4	Agriculture et Agroalimentaire Canada
4	Agence canadienne d'inspection des aliments
4	Affaires indiennes et du Nord Canada
4	Secrétariat du Conseil du Trésor du Canada
3	Commission des plaintes du public contre la GRC
3	Environnement Canada
3	Commission de la fonction publique du Canada
2	Centre des armes à feu Canada
2	Société canadienne d'hypothèques et de logement
2	Agence de la fonction publique du Canada
2	Ombudsman de la Défense nationale et des Forces canadiennes
1	Société Radio-Canada
1	Comité des griefs des Forces canadiennes
1	Commission canadienne des droits de la personne
1	Office des transports du Canada
1	Enquêteur correctionnel Canada
1	Exportation et développement Canada
1	Centre d'analyse des opérations et déclarations financières du Canada
1	Commission de l'immigration et du statut de réfugié du Canada
1	Industrie Canada
1	Bureau de l'inspecteur général du Service canadien du renseignement de sécurité
1	Musée des sciences et de la technologie du Canada
1	Commission nationale des libérations conditionnelles
1	Ressources naturelles Canada
1	Commission d'appel des pensions du Canada
1	Sécurité publique Canada
1	Commission des relations de travail dans la fonction publique
1	Tribunal de la dotation de la fonction publique
1	Monnaie royale canadienne
1	Statistique Canada
1	Anciens Combattants Canada
759	Total

Vous trouverez une définition des types de plaintes à l'annexe 1.

En raison de leur mandat, certaines institutions détiennent une quantité considérable de renseignements personnels. Elles sont donc plus susceptibles de recevoir de nombreuses demandes d'accès à ces renseignements personnels et des plaintes subséquentes.

Total	759	292	295	172
Autres	117	49	29	39
Justice Canada	18	4	13	1
international				
Affaires étrangères et Commerce	27	6	7	14
Société canadienne des postes	28	16	8	4
Agence du revenu du Canada	38	18	9	11
de sécurité				
Service canadien du renseignement	45	44	0	1
Défense nationale	48	17	19	12
Service Canada	52	13	14	25
Agence des services frontaliers du Canada	54	18	31	5
Gendarmerie royale du Canada	84	59	14	11
Service correctionnel du Canada	248	48	151	49
Total		accès aux renseignements personnels	Délais	Protection des renseignements personnels

Les dix institutions ayant reçu le plus de plaintes

Vous trouverez une définition des types de plaintes à l'annexe 1.

Comme au cours des exercices précédents, les plaintes les plus fréquentes soumisees au Commissariat concernaient l'accès aux renseignements personnels et la durée que les ministères et les organismes gouvernementaux prennent pour répondre aux demandes d'accès.

Type de plainte	Nombre	Pourcentage
Accès	292	38
Délais	259	34
Utilisation et communication	124	16
Collecte	33	4
Correction – délais	26	3
Avis de prorogation	10	1
Conservation et retrait	9	1
Correction – annotation	5	1
Langue	1	< 1
Total	759	

Plaintes reçues par type

ANNEXE 3

STATISTIQUES 2007-2008 SUR LES DEMANDES DE RENSEIGNEMENTS, LES PLAINTES ET LES ENQUÊTES EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Demandes de renseignements

Le service des demandes de renseignements a reçu plus de 4 000 demandes de renseignements concernant la *Loi sur la protection des renseignements personnels* entre le 1^{er} avril 2007 et le 31 mars 2008.

Certaines des questions les plus fréquemment posées avaient trait à la façon de présenter des demandes officielles d'accès aux renseignements personnels et à la procédure pour déposer une plainte contre les institutions gouvernementales qui, par exemple, dépassent les délais prescrits et ne se conforment pas à la *Loi sur la protection des renseignements personnels*. Nous avons également reçu des demandes de renseignements de personnes qui demandaient conseil au Commissariat après avoir subi diverses atteintes à leur vie privée.

Demandes de renseignements en vertu de la Loi sur la protection des renseignements personnels reçues par le service des demandes de renseignements	
Demandes téléphoniques	2 199
Demandes écrites (lettres, courriels, télécopies)	2 059
Nombre total de demandes de renseignements reçues	4 258

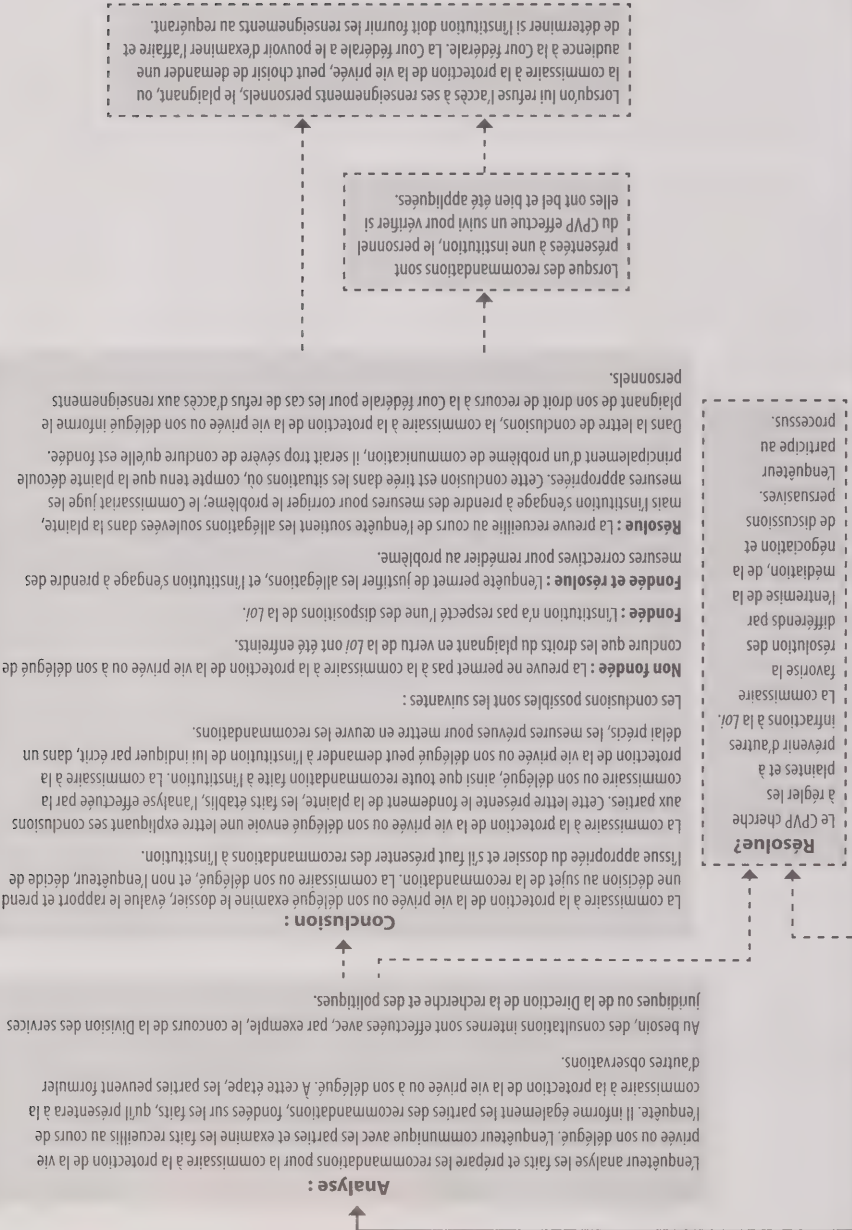
Demandes de renseignements en vertu de la Loi sur la protection des renseignements personnels fermées	
Demandes téléphoniques	2 221
Demandes écrites (lettres, courriels, télécopies)	1 901
Nombre total de demandes de renseignements fermées	4 122

Demandes générales de renseignements reçues*	
Demandes téléphoniques	2 231
Demandes écrites (lettres, courriels, télécopies)	136
Nombre total de demandes de renseignements reçues	2 367

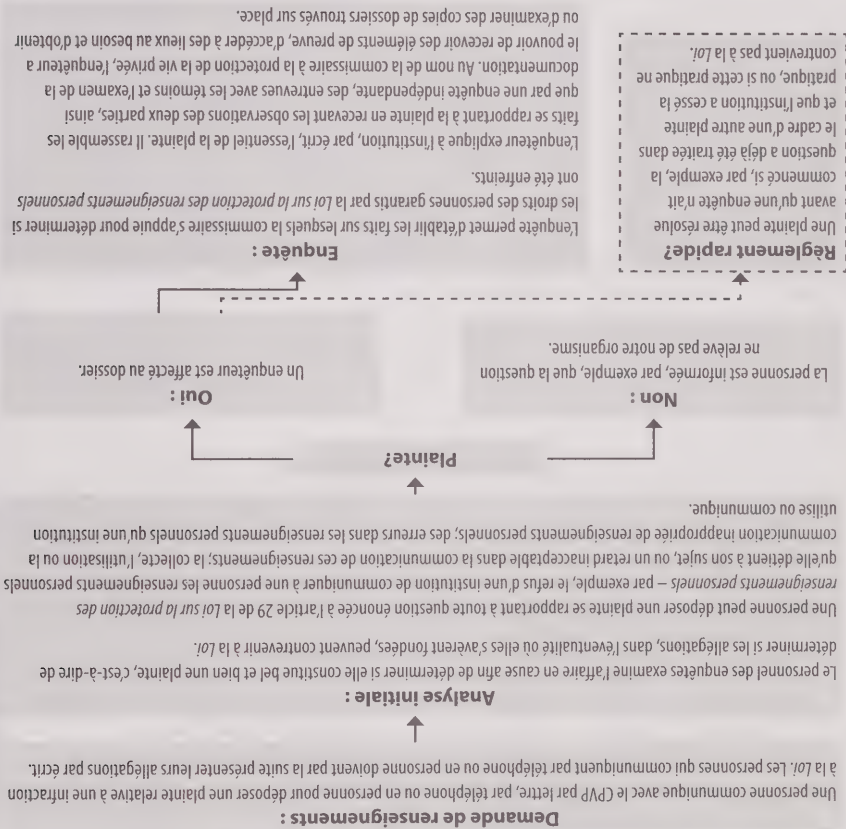
Demandes générales de renseignements fermées	
Demandes téléphoniques	2 229
Demandes écrites (lettres, courriels, télécopies)	140
Nombre total de demandes de renseignements fermées	2 369

* Il s'agit de demandes de renseignements relatives à la protection des renseignements personnels, mais elles ne peuvent être liées ni à la LPRP ni à la LPRPDE.

Note : une ligne discontinue (- - -) indique un résultat possible.



PROCESSUS D'ENQUÊTE EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS



Note : une ligne discontinue (---) indique un résultat possible.

Fondée : L'Institution fédérale n'a pas respecté les droits d'une personne aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée et résolue : Les allégations sont corroborées par l'enquête et l'Institution fédérale accepte de prendre des mesures correctives afin de remédier à la situation.

Résolue : Après une enquête approfondie, le CPVP a participé à la négociation d'une solution satisfaisant les deux parties. Cette conclusion est réservée aux plaignantes qu'on pourrait difficilement qualifier de fondées du fait que la situation relève essentiellement d'une mauvaise communication ou d'un malentendu.

Réglée en cours d'enquête : Le CPVP a participé à la négociation d'une solution satisfaisant toutes les parties dans le cadre de l'enquête. Aucune conclusion n'est rendue.

Abandonnée : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons. Par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire, ou il est impossible de le trouver afin qu'il fournisse des renseignements supplémentaires essentiels pour arriver à une conclusion.

nationales et publiées dans *Info Source* : ils sont détruits trop rapidement ou conservés trop longtemps.

En outre, les renseignements personnels utilisés à des fins administratives doivent être conservés pendant au moins deux ans après la dernière application d'une mesure administrative, à moins que la personne n'ait consenti à leur retrait.

- **Utilisation et communication** – Des renseignements personnels sont utilisés ou communiqués sans le consentement de la personne concernée et ne satisfont pas à l'un des critères d'utilisation ou de communication permise sans consentement énoncés aux articles 7 et 8 de la *Loi*.

Délais

- **Délais** – L'institution n'a pas répondu dans les délais prescrits.
- **Avis de prorogation** – L'institution n'a pas donné une justification appropriée pour la prorogation; elle a fait la demande de prorogation après le délai initial de 30 jours ou elle a fixé l'échéance à plus de 60 jours de la date de réception de la demande.

- **Correction/annotation – délais** – L'institution n'a pas corrigé les renseignements personnels ou n'a pas annoté le dossier dans les 30 jours suivant la réception de la demande de correction.

DEFINITIONS DES CONCLUSIONS ET D'AUTRES DISPOSITIONS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le CPVP a élaboré une série de définitions des conclusions qui expliquent les résultats des enquêtes qu'il effectue en vertu de la *Loi sur la protection des renseignements personnels*.

Réglée rapidement : S'applique aux cas où l'affaire est réglée avant même qu'une enquête officielle ne soit entamée. Par exemple, si une personne dépose une plainte dont le sujet a déjà fait l'objet d'une enquête par le CPVP et a été considéré conforme à la *Loi sur la protection des renseignements personnels*, nous expliquons la situation à cette personne. Il nous arrive également de recevoir des plaintes pour lesquelles une enquête officielle aurait pu avoir des conséquences défavorables pour la personne. En pareil cas, nous expliquons en détail la situation au plaignant. Si ce dernier décide de ne pas poursuivre l'affaire, celle-ci est jugée « réglée rapidement ».

Non fondée : L'enquête n'a pas permis de déceler des éléments de preuve qui suffisent à conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant selon la *Loi sur la protection des renseignements personnels*.

DEFINITIONS DES TYPES DE PLAINTES

Les plaintes adressées au CPVP sont réparties en trois grandes catégories :

Accès

- **Accès** – Une personne n'a pas obtenu tous les renseignements personnels qu'une institution détient à son sujet parce qu'il manque des documents ou des renseignements, ou encore parce que l'organisation a invoqué des exceptions afin de ne pas communiquer les renseignements.

- **Correction/annotation** – L'institution n'a pas apporté les corrections aux renseignements personnels ou ne les a pas annotés parce qu'elle n'approuve pas les corrections demandées.

- **Langue** – Les renseignements personnels n'ont pas été fournis dans la langue officielle demandée.

- **Frais** – Des frais ont été exigés pour répondre à la demande de renseignements effectuée en vertu de la *Loi sur la protection des renseignements personnels*, alors qu'aucun frais n'est actuellement prévu pour l'obtention de renseignements personnels.

- **Répertoire** – *Info Source*, un répertoire du gouvernement fédéral qui décrit chaque institution et les banques de données – groupes de fichiers sur un même sujet – que l'institution possède, ne décrit pas de façon adéquate le fonds de renseignements personnels que détient une institution.

Protection des renseignements personnels

- **Collecte** – Une institution a recueilli des renseignements personnels qui ne sont pas nécessaires à l'exploitation d'un de ses programmes ou à l'une de ses activités; les renseignements personnels n'ont pas été recueillis directement auprès de la personne concernée; ou la personne n'a pas été informée des fins pour lesquelles les renseignements personnels ont été recueillis.

- **Conservation et retrait** – Des renseignements personnels ne sont pas conservés selon les calendriers de conservation et de retrait approuvés par les Archives

- **Intégrité et protection de l'identité, vol d'identité**

- Améliorer les pratiques de gestion des renseignements personnels des organisations.
- Sensibiliser davantage le grand public à la protection de l'identité.
- Promouvoir une approche concertée du gouvernement fédéral en matière de protection de l'identité.

- **Renseignements génétiques**

- Favoriser la recherche et le développement des connaissances pour relever les nouveaux défis posés par la génétique dans le contexte des régimes conventionnels de protection des données.
- Accroître la sensibilisation du grand public aux utilisations possibles des renseignements génétiques.

Le Commissariat a déterminé les quatre autres grandes priorités organisationnelles suivantes :

- Continuer d'améliorer la prestation des services grâce à la convergence des efforts et à l'innovation, y compris l'adoption de nouvelles stratégies d'enquête pour améliorer l'efficacité de notre processus de résolution des plaintes.
- Renforcer la capacité organisationnelle de manière durable en élargissant le Commissariat et en poursuivant un projet de renouvellement de la gestion de l'information.

- Aider les Canadiennes et les Canadiens à prendre des décisions plus éclairées au moyen d'initiatives d'éducation du public d'envergure comme une campagne de marketing social sur la protection de la vie privée des enfants en ligne et des programmes de sensibilisation en partenariat avec les commissaires à la protection de la vie privée des provinces et des territoires.

- **Promouvoir stratégiquement la protection de la vie privée à l'échelle mondiale pour les Canadiennes et les Canadiens en travaillant avec des**

organisations comme l'Organisation de coopération et de développement économiques (OCDE) et la Coopération économique de la zone Asie-Pacifique (APEC).

La liste des enjeux que le Commissariat à la protection de la vie privée aborde quotidiennement demeure toujours très longue. Dans le but de concentrer nos efforts sur les menaces les plus importantes au droit à la vie privée des Canadiennes et des Canadiens, nous avons dégagé quatre grandes priorités stratégiques : technologies de l'information, sécurité nationale, intégrité et protection de l'identité, et renseignements génétiques.

Au cours de 2008-2009, un objectif clé du Commissariat consistera à **exercer un rôle de chef de file dans nos dossiers prioritaires**. Nos plans pour faire face à ces menaces comprennent les étapes suivantes :

• Technologies de l'information

- Développer une capacité suffisante pour évaluer les répercussions des nouvelles technologies de l'information sur la protection de la vie privée.
- Sensibiliser davantage le grand public aux technologies ayant possiblement une incidence sur la protection de la vie privée.
- Fournir une orientation pratique aux organisations sur la mise en œuvre de technologies particulières.

• Sécurité nationale

- Nous assurer que les mesures relatives à la sécurité nationale protègent convenablement la vie privée.
- Surveiller adéquatement, chez les organismes chargés de la sécurité nationale, les pratiques de gestion des renseignements personnels et voir à ce que ces organismes se responsabilisent.
- Sensibiliser davantage le grand public à l'incidence sur la vie privée des initiatives en matière de sécurité nationale.

particulier, ainsi que les exigences plus rigoureuses des principaux décideurs pour repérer l'information fiable concernant les répercussions sur la vie privée des thèmes abordés lors de la Conférence. Ces cahiers, qui constituent un legs important de la Conférence, sont accessibles sur notre site Web consacré à celle-ci à l'adresse suivante : www.conferencevieprivée2007.gc.ca.

Nous avons affiché les détails du coût de la Conférence sur notre site Web. Nous sommes bien à l'intérieur de nos objectifs financiers globaux.

félicitations de la part des participants ont justifié le temps et les ressources investis dans cet événement.

Le thème de la Conférence était « Les horizons de la protection de la vie privée : Terra incognita ». Les anciens cartographes utilisaient ce mot latin pour désigner les territoires inconnus qu'il restait à délimiter sur une carte. Sur l'un des premiers globes terrestres connus de l'Europe, on peut lire sur un bord non cartographié de l'océan « hic sunt dracones », ce qui veut dire « Ici résident les dragons ».

Cette notion de paysage inconnu avec des dragons qui rôdent semblait la métaphore parfaite pour l'avenir de la protection de la vie privée. Les enjeux relatifs à la protection de la vie privée changent rapidement; l'arrivée de nouvelles technologies et la guerre internationale au terrorisme agissant comme forces pouvant menacer la vie privée des gens autour du monde.

Le but de notre conférence était de commencer à brosser un tableau de ce à quoi pourrait ressembler demain le monde de la protection de la vie privée et aussi d'équiper les défenseurs du droit à la vie privée de quelques solides instruments pour tuer les dragons. Durant une série de plénières, d'ateliers et de séances d'information, nous avons examiné les meilleures stratégies par lesquelles défendre le droit à la vie privée dans un contexte de changements constants.

Les participants ont entendu les grands noms de la protection de la vie privée, y compris : Bruce Schrier, gourou en technologie de la sécurité et auteur, Simon Davies, pionnier sur la scène internationale de la protection de la vie privée et fondateur de Privacy International, Katharine Albrecht, défenseur de la vie privée des consommateurs; Marc Rotenberg, directeur exécutif du Electronic Privacy Information Center; Peter Fleischer, conseiller en matière de protection internationale des renseignements personnels pour Google; Peter Hustinx, contrôleur européen de la protection des données; Peter Schaar, président sortant du Groupe de travail sur la protection des données établi en vertu de l'article 29 de l'UE; enfin, Alex Türk, de la France, qui assume actuellement la présidence du Groupe. Notre invité d'honneur, qui a lancé la Conférence, était l'honorable Peter Milliken, président de la Chambre des communes.

Le programme de la Conférence mettait en relief le vaste éventail d'enjeux qui auront une incidence sur la protection de la vie privée dans les années à venir ainsi que la nature de plus en plus mondiale des questions de protection de la vie privée.

Nous avons préparé 14 cahiers de consultation avant la Conférence. La plupart incluaient un document commandé à un expert en la matière et diverses autres ressources, comme des documents de recherche et du matériel bibliographique, pour satisfaire la curiosité des participants qui peuvent être des profanes dans un domaine

à l'information étaient non fondées et que la troisième avait été résolue. Le commissaire à l'information a aussi conclu qu'une des plaintes qui visait les délais n'était pas fondée et que l'autre était résolue.

Le CPVP a reçu 45 demandes de renseignements personnels en vertu de la LPRP. Il en a transféré 23 aux institutions fédérales qui détenaient les renseignements demandés et il a répondu à 22 demandes d'accès aux renseignements du CPVP. Toutes ces demandes ont été traitées dans les délais prescrits.

Le Commissariat a reçu deux plaintes, en vertu de la LPRP, d'une personne qui alléguait un refus d'accès. Les plaintes ont été présentées dans le cadre d'un processus indépendant et ont été jugées non fondées en avril 2008.

La Loi fédérale sur la responsabilité ne comporte aucun mécanisme pour examiner les plaintes en vertu de la LPRP qui visent le CPVP. Puisqu'il serait totalement inapproprié que le CPVP enquête sur sa propre administration de la LPRP, il a créé le poste de « commissaire spécial à la protection de la vie privée ».

En septembre 2007, l'honorable juge Peter Cory a été engagé à titre de commissaire spécial à la protection de la vie privée. La commissaire à la protection de la vie privée lui a délégué la majorité de ses pouvoirs, de ses responsabilités et de ses fonctions prévus aux articles 29 à 35 et à l'article 42 de la *Loi*. Le juge Cory a terminé son contrat en mars 2008. Un nouveau commissaire spécial à la protection de la vie privée, le juge Andrew MacKay, assume ces fonctions depuis.

De nombreuses demandes reçues en vertu de la *Loi sur l'accès à l'information* et de la LPRP concernaient le contenu de dossiers d'enquête du CPVP. Dans quelques cas, le contenu des dossiers n'a pas été communiqué, comme le prescrivent ces deux lois, parce que l'enquête ou les actions en justice étaient en cours. Dans les cas où l'enquête était terminée, le contenu du dossier a été traité et l'accès a été octroyé sous réserve des exceptions applicables.

CONFÉRENCE INTERNATIONALE

Tel qu'il est mentionné dans le rapport annuel de 2007 sur la LPRPDE, le succès de la 29^e Conférence internationale des commissaires à la protection des données et de la vie privée – qui s'est déroulée à Montréal en septembre et faisait suite à notre engagement pris en 2002 – a dépassé nos attentes les plus élevées.

Nous avons accueilli plus de 600 commissaires, universitaires, spécialistes de la protection de la vie privée, défenseurs des droits, responsables gouvernementaux, spécialistes de la TI et autres de partout dans le monde – ce qui en a fait la plus grande conférence du genre jamais organisée. Qui plus est, les commentaires positifs et les

Dans une décision rendue en février 2008, le juge Gibson a accepté la prémisse fondamentale suivante, établie par la Cour suprême du Canada : dans une situation mettant en jeu des renseignements personnels sur une personne, le droit au respect de la vie privée l'emporte sur le droit d'accès à l'information.

Il a également adopté le critère juridique proposé par le Commissariat : « Un renseignement concerne un individu identifiable lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles ».

En se fondant sur la preuve qui lui a été soumise, le juge Gibson a conclu que la communication de la province augmenterait considérablement le risque qu'une personne puisse être identifiée, compte tenu de tous les champs de données déjà communiqués à partir de la base de données et de la combinaison possible avec d'autres renseignements accessibles au public, comme les notices nécrologiques. Cela est particulièrement vrai pour les rapports concernant une seule personne ou un très petit groupe dans les provinces et les territoires plus petits.

Ainsi, dans les circonstances, le nom de la province est une donnée qui constitue un renseignement personnel, auquel l'accès a été refusé à juste titre.

Il convient également de noter que le juge a insisté sur l'importance du pouvoir discrétionnaire du ministre dans la décision de communiquer ou non exceptionnellement de tels renseignements personnels dans l'intérêt public. Dans le cas présent, le ministre a considéré avec justesse les faits qui lui ont été soumis et a trouvé que l'intérêt public d'une telle communication ne l'emporterait pas clairement sur le risque d'atteinte à la vie privée.

SECTION DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le Commissariat a maintenu un exercice complet durant lequel il a été assujéti à la *Loi sur l'accès à l'information* et à la *LPRP*. (La *Loi fédérale sur la responsabilité* a modifié ces deux lois afin qu'elles s'appliquent au Commissariat.)

Le CPVP a reçu 44 demandes officielles en vertu de la *Loi sur l'accès à l'information*. Il en a transféré 14 aux institutions fédérales responsables des documents recherchés et il a traité 29 demandes relatives à l'accès à l'information. Une demande a été reportée. Toutes les demandes ont été traitées dans les délais prescrits.

Le Commissariat a reçu cinq plaintes de deux personnes en vertu de la *Loi sur l'accès à l'information* – trois d'entre elles concernent le refus d'accès et les deux autres portent sur les délais. Le commissaire a jugé que deux des plaintes relatives à l'accès

En vertu de l'article 41 de la *Loi*, le demandeur a exercé un recours en révision des conclusions de la commissaire à la protection de la vie privée. Cependant, l'objectif d'appliquer cet article est de demander à la Cour de déterminer si l'institution fédérale visée par la plainte a respecté les dispositions applicables de la *Loi* lorsqu'elle a refusé de donner accès aux renseignements personnels demandés par le plaignant. L'article ne prévoit pas de recours contre la commissaire à la protection de la vie privée.

Le juge Blanchard a conclu qu'il est clair que la commissaire à la protection de la vie privée n'a aucun pouvoir décisionnel et que les conclusions et les recommandations formulées à la suite d'une enquête en vertu de la *Loi* n'ont aucune force exécutoire sur l'institution fédérale.

Il a également souligné que, selon la *Loi*, il est clair qu'il n'incombe pas à la commissaire à la protection de la vie privée de justifier un refus, mais que cette responsabilité revient à l'institution ayant refusé de donner accès aux renseignements personnels demandés.

La Cour a donc accueilli la décision de la commissaire à la protection de la vie privée, ordonnant que la révision judiciaire ne soit réalisée que si le demandeur soumet une nouvelle demande auprès du SCRS, ce qui a été fait en mars 2008.

Intervention dans une affaire touchant la Loi sur l'accès à l'information

X. c. Ministre de la Santé au Canada
Dossier de la Cour fédérale T-347-06

Comme il a été mentionné dans le rapport annuel 2006-2007, la commissaire à la protection de la vie privée a obtenu le statut d'intervenant dans une cause initiée en vertu de la *Loi sur l'accès à l'information* qui soulevait d'importantes questions de protection de la vie privée. Le Commissariat s'inquiétait du risque que des personnes soient identifiées lorsque des renseignements gouvernementaux sont combinés à des renseignements accessibles au public.

Le demandeur, un producteur de la CBC, a voulu accéder au système canadien d'information sur les effets indésirables des médicaments de Santé Canada – une base de données de renseignements sur les effets indésirables présumés de produits de santé commercialisés au Canada.

En réponse à cette demande, Santé Canada a communiqué certains renseignements, mais a refusé de dévoiler le nom des provinces où les données sur les effets indésirables des médicaments avaient été recueillies, justifiant sa décision par le fait qu'il s'agissait de renseignements personnels aux termes de la LPPR.

DEVANT LES TRIBUNAUX

À l'instar des années précédentes, très peu de cas ont été portés devant les tribunaux aux termes de la LPRP en 2007-2008.

En vertu de l'article 41 de la Loi sur la

protection des renseignements personnels, la Cour fédérale ne peut se pencher que sur le refus d'une institution fédérale de communiquer les renseignements personnels demandés en vertu de la Loi.

Un individu ne peut appliquer l'article 41

en cas de collecte, d'utilisation ou de communication injustifiée de ses renseignements personnels par une institution gouvernementale.

Le Commissariat a demandé au gouvernement fédéral d'étendre les motifs de recours aux tribunaux en vertu de l'article 41 de la LPRP à toute la gamme des protections et des droits relatifs à la vie privée que cette loi garantit. Il a également recommandé qu'on autorise la Cour fédérale à allouer des dommages et intérêts à la charge des institutions contrevenantes.

Tant que la Loi ne sera pas modifiée, le nombre de cas portés devant les tribunaux demeurera très faible.

Les cas d'intérêt suivants ont été portés devant la Cour fédérale en 2007-2008.

Conformément à l'esprit de notre mandat, nous ne publions pas le nom des plaignants afin de respecter leur vie privée. Nous rénumérons que le numéro du greffe et le nom de l'institution fédérale en cause.

X. c. Commissariat à la protection de la vie privée du Canada
Dossier de la Cour fédérale T-1903-07

Le demandeur a porté plainte contre le Service canadien du renseignement de sécurité (SCRS) pour n'avoir pas fourni les renseignements personnels demandés. La commissaire à la protection de la vie privée a jugé que cette plainte était non fondée.

Permis de conduire amélioré (PCA) de l'Agence des services frontaliers du Canada

Le CPVP a travaillé avec le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique pendant l'examen du projet pilote du permis de conduire amélioré entre cette province et l'État de Washington. L'Agence des services frontaliers du Canada encourage ce projet pilote ainsi que les projets de PCA d'autres provinces, et elle participe à leur coordination. Le PCA est proposé comme solution de rechange au passeport canadien pour les voyageurs qui entrent aux États-Unis par les frontières terrestres. Ce projet fait suite aux nouvelles règles du gouvernement des États-Unis qui exigent des preuves d'identité et de citoyenneté.

Dans le cadre du projet pilote de la Colombie-Britannique, l'Agence des services frontaliers du Canada recueille les renseignements des demandeurs de la province et les transfère à la U.S. Customs and Border Protection.

L'une des préoccupations soulevées par le Commissariat lors de l'examen de l'EFVP concerne la répétition du processus de vérification des renseignements personnels et des données déjà en place à Passeport Canada. D'autres préoccupations concernent les points suivants : le cadre légal flou de la vérification de la citoyenneté, le consentement valable, l'utilisation potentielle des renseignements personnels par le gouvernement des États-Unis, l'utilisation du PCA à d'autres fins ainsi que les risques pour la protection des renseignements personnels associés aux étiquettes d'identification par radiofréquence (IRF).

Le CPVP a pressé l'Agence des services frontaliers du Canada de fournir l'assurance que les prochains projets de PCA n'iront pas de l'avant de manière permanente, à moins que les renseignements personnels des conducteurs demeurent au Canada et que les renseignements que contient le PCA ne servent à aucune autre fin que traverser la frontière. Au moment de la rédaction du présent rapport, la manière dont les renseignements seront communiqués aux autorités américaines faisait toujours l'objet de discussions, mais l'Agence des services frontaliers du Canada a fait savoir que la base de données, elle-même, demeurera au Canada.

Système national intégré d'information interorganismes de la GRC et de Sécurité publique Canada

Le système national intégré d'information interorganismes (N-III) est un programme de partage de dossiers électronique qui relie les services de police nationaux, provinciaux et municipaux, et qui comporte des fonctions permettant d'étendre l'accès aux ministères fédéraux et de partager des renseignements avec eux.

L'initiative est un partenariat de la GRC, de Sécurité publique Canada et de nombreux ministères et organismes, comme l'Agence des services frontaliers du Canada, le ministère de la Citoyenneté et de l'Immigration, le Centre des armes à feu Canada, le Service correctionnel du Canada et la Commission nationale des libérations conditionnelles.

Étant donné le grand nombre d'institutions participantes, le CPVP a demandé à Sécurité publique Canada d'élaborer une EFPV globale qui inclurait un cadre de gestion de la protection de la vie privée avec des normes et des limites mesurables pour tous les organismes gouvernementaux qui ont accès à des renseignements et qui les partagent grâce à des systèmes comme le Portail national d'informations policières.

Le Commissariat avait espoir qu'une telle EFPV permettrait de donner un aperçu de l'analyse de rentabilisation complète établissant et justifiant la nécessité d'échanger davantage de renseignements; de rédiger un engagement de Sécurité publique Canada à protéger les renseignements personnels; de fixer des normes mesurables pour les vérifications de conformité au sein de chaque ministère de portefeuille; et d'inclure une stratégie de communication pour informer les citoyens de la manière dont ce programme peut mener à la communication de leurs renseignements personnels à des institutions gouvernementales.

Un an après en avoir fait la demande, le Commissariat attend toujours l'EFPV globale, mais il a été informé au printemps 2008 que le travail venait d'être entrepris.

téléphoniques dans les ports canadiens et le processus de traitement des demandes de passeport aux bureaux de Service Canada.

Dans la plupart des cas, le CPVP a mis au jour des risques pour la vie privée et a émis des recommandations, lesquelles sont habituellement prises au sérieux.

Exemples d'examen d'EFFVP

Programme de protection des passagers (liste des personnes interdites de vol) de Transports Canada

Si le Commissariat continue d'avoir de sérieuses inquiétudes à propos des risques pour la protection des renseignements personnels que pose la liste des personnes interdites de vol, l'examen de l'EFFVP du programme de Transports Canada a entraîné quelques améliorations. Par exemple, dans la foulée des recommandations du CPVP, Transports Canada a mis en place nos suggestions sur les procédures de recours pour les passagers, a effectué une vérification de l'efficacité du programme, a prévu des clauses de confidentialité dans les protocoles d'entente, et a instauré des normes d'intervention pour la GRC et le Service canadien du renseignement de sécurité (SCRS) lorsqu'une personne se voit refuser l'embarquement à bord d'un avion. Cependant, la recommandation de ne pas communiquer aux services de police locaux les renseignements personnels des personnes auxquelles l'embarquement a été refusé n'a pas été entièrement mise en œuvre.

De plus, la recommandation de soumettre le Programme de protection des passagers ainsi que d'autres listes de surveillance à un examen par une commission parlementaire dans un forum ouvert et transparent a été rejetée.

Enquête canadienne sur les mesures de la santé de Statistique Canada

L'enquête canadienne sur les mesures de la santé permet de recueillir des renseignements sur la santé générale et les habitudes de vie des citoyens. Notre rapport d'examen de cette enquête déconseillait initialement la conservation prévue d'échantillons de sang, d'urine et d'ADN des participants pour une durée indéterminée à des fins d'études éventuelles non précises. Le Commissariat juge que cette pratique vide de son sens le consentement que les participants donnent pour la collecte des échantillons.

Le CPVP a recommandé à Statistique Canada de stocker les échantillons biologiques, selon un code anonyme, pour une période déterminée n'excédant pas 20 ans. Il a également recommandé que l'enquête n'offre pas de garder à long terme les échantillons biologiques des répondants de 6 à 13 ans, dont le consentement doit être donné par un des parents ou par le tuteur.

Statistique Canada a décidé de mettre à exécution son plan de stockage illimité. Il a proposé qu'un comité de surveillance, composé de parties intéressées comme le CPVP, puisse étudier les façons dont les échantillons stockés pourraient être utilisés dans le futur. Le plan de stockage des échantillons biologiques des jeunes sujets sera également mis en œuvre; toutefois, l'organisme communiquera avec eux après leur 14^e anniversaire pour obtenir un consentement explicite.

Examen des évaluations des facteurs relatifs à la vie privée

L'évaluation des facteurs relatifs à la vie privée (EFVP) est un outil de gestion important pour aider les institutions fédérales à déterminer et à atténuer les risques pour la vie privée avant la mise en œuvre d'un programme.

L'EFVP – obligatoire en vertu d'une politique du Secrétaire du Conseil du Trésor – est destinée à encourager les ministères à placer la protection de la vie privée au centre de leurs préoccupations lorsqu'ils mettent en œuvre de nouveaux programmes et de nouvelles initiatives. Le CPVP croit que les EFVP devraient être obligatoires en vertu de la LPRP (pour de plus amples renseignements, voir p. 48).

La Direction de la vérification et de la revue a examiné les EFVP qui lui ont

été soumises afin d'évaluer les risques pour la vie privée des programmes et des services fédéraux, et elle a fourni des conseils le cas échéant. Ainsi, le CPVP peut s'assurer que des mesures de protection des renseignements personnels sont incorporées aux programmes et systèmes.

Le Commissariat est satisfait de constater que, de plus en plus, les ministères invitent des représentants du CPVP aux réunions préliminaires tenues durant la phase d'élaboration des EFVP, et parfois même avant. Cette participation permet au Commissariat de suggérer des pratiques optimales et de faire rapidement des mises en garde concernant les risques pour la vie privée que peuvent poser les nouveaux programmes et initiatives.

Une des grandes priorités de cette direction en 2007-2008 était de réduire les retards dans l'examen des EFVP. Pendant l'année, l'arriéré de demandes en attente a beaucoup diminué, passant de 50 à 18.

La Direction a examiné 78 EFVP de nombreux programmes et initiatives fédéraux. Certaines concernaient des projets controversés et médiatisés, comme la liste des personnes interdites de vol de Transports Canada et le permis de conduire amélioré de l'Agence des services frontaliers du Canada. Le Commissariat a également examiné les risques pour la vie privée d'initiatives moins connues : un nouveau programme de prestations pour les anciens combattants, l'enregistrement des conversations

Les EFVP en chiffres

60	Nouvelles EFVP soumises au CPVP
78	EFVP examinées et lettres de recommandations envoyées aux ministères (y compris les EFVP d'années précédentes)
434	Recommandations du CPVP aux ministères
239	Demandes aux ministères concernant l'information manquante dans les EFVP

Utilisation du numéro d'assurance sociale

Le Secrétaire du Conseil du Trésor a fait savoir au CPVP qu'il tiendra compte de la question des courtiers en données dans la révision de sa Politique d'évaluation des facteurs relatifs à la vie privée qui devrait être terminée d'ici avril 2009.

En juin 2007, un prestataire de la Sécurité de la Vieillesse a écrit à la commissaire pour lui faire part de son inquiétude à propos de la présence du numéro d'assurance sociale sur sa carte d'identité de la Sécurité de la Vieillesse. Le citoyen indiquait que cet ajout force les citoyens âgés à révéler un renseignement personnel sensible chaque fois qu'ils utilisent leur carte pour obtenir des privilèges et des réductions.

La lettre demandait au Commissariat de communiquer avec Ressources humaines et Développement social Canada pour soulever le problème. Quelques mois plus tard, le Ministère a informé le CPVP que le numéro d'assurance sociale ne serait plus imprimé sur la carte.

Le numéro d'assurance sociale a été créé en 1964 afin de servir de numéro de compte pour le Régime de pensions du Canada et divers programmes d'assurance-emploi. En 1967, l'Agence du revenu du Canada (ARC) de l'époque a instauré l'utilisation du numéro d'assurance sociale aux fins de déclaration de revenus.

Une étude récente du CPVP a permis de découvrir que plus de 70 ministères et organismes fédéraux utilisent le numéro d'assurance sociale d'une façon ou d'une autre. De plus, les divers usages du numéro d'assurance sociale figurent dans environ 170 lois provinciales.

Malgré des années d'effort de la part des gouvernements, du Commissariat, des autres commissaires à la protection de la vie privée, des défenseurs de la vie privée et des citoyens pour restreindre l'utilisation du numéro d'assurance sociale, au cours des années l'usage a fait boucle de neige à tel point que beaucoup y voient dans les faits un numéro de client ou même un numéro d'identité nationale.

Parallèlement, aucune disposition législative ne prévoit de protection en ce qui concerne l'utilisation du numéro d'assurance sociale. Il s'agit d'une préoccupation sérieuse puisque ce numéro est la clé de voûte des renseignements personnels d'une personne — les voleurs l'utilisent pour demander des cartes de crédit et ouvrir des comptes bancaires. Le Secrétaire du Conseil du Trésor a publié récemment une nouvelle politique régissant l'utilisation du numéro d'assurance sociale. Reste à voir si elle arrivera à en restreindre l'utilisation.

Le forage de données et le secteur public

La façon dont les courtiers en données recueillent, utilisent et communiquent des renseignements personnels est une de nos préoccupations des dernières années. De même, des enjeux concernant la vie privée ont été mis en relief dans nombre d'études et d'incidents importants impliquant des courtiers en données.

Vers la fin de 2006, *le Ottawa Citizen* a publié un article décrivant la manière dont la GRC avait acheté des renseignements personnels à des courtiers en données commerciales depuis de nombreuses années et les avait conservés. La révélation a non seulement suscité des questions sur la manière dont la GRC utilisait ces renseignements, mais elle a également soulevé la question de savoir si d'autres institutions fédérales achètent ce type de renseignements.

Les courtiers en données recueillent et analysent des renseignements personnels – qu'il s'agisse de renseignements financiers, de renseignements médicaux ou de données sur le crédit – afin de concevoir et de vendre des produits de données, souvent à des spécialistes du marketing. Du point de vue de la protection de la vie privée, le CPVP se préoccupe de l'exactitude de ce type de données ainsi que du risque de faire des suppositions erronées sur les personnes.

La GRC a informé le Commissariat qu'elle a des ententes contractuelles avec des courtiers en données qui fournissent des rapports commerciaux sur des sociétés publiques et privées ainsi que des coordonnées (adresses et numéros de téléphone) de consommateurs et d'entreprises.

Selon le mandat de la section opérationnelle, la GRC fait plus ou moins appel aux courtiers en données. Par exemple, les sections des infractions commerciales peuvent préparer des profils économiques sur des personnes ou des entreprises dans le cadre d'enquêtes sur des faillites.

La GRC nous a expliqué que l'information fournie par les courtiers en données complète son travail de renseignement et d'enquête, et qu'elle est considérée comme une source secondaire de renseignements dont la pertinence, l'exactitude et la fiabilité sont indéterminées. Le CPVP en comprend que rien n'est entrepris en fonction de ces seuls renseignements.

Le Commissariat a réalisé un sondage restreint pour évaluer l'utilisation des services des courtiers en données au sein d'autres institutions fédérales et il a conclu que cet usage ne semble pas répandu.

Les personnes dont le nom figure dans les fichiers inconsultables de la GRC risquent de subir de graves préjudices. Par exemple, elles risquent d'avoir des difficultés à obtenir une cote de sécurité pour leur travail ou à passer la frontière.

Plus de la moitié des dossiers examinés dans le cadre de la vérification des fichiers inconsultables n'auraient pas dû s'y trouver. À titre d'exemple, un dossier vieux de sept ans trouvé parmi le fichier inconsultable sur la sécurité nationale concernait la dénonciation d'un résident qui avait informé les autorités qu'un homme s'était rendu dans une maison de chambres et qu'il pouvait s'agir d'une affaire de drogues. Le fichier indiquait qu'après enquête, la police avait découvert que l'homme n'avait fait que déposer sa fille dans une école du voisinage et qu'il était sorti de sa voiture pour fumer.

La commissaire à la protection de la vie privée s'est dite convaincue que la GRC considère avec sérieux ses recommandations et qu'elle prendra des mesures pour veiller à ce que les fichiers inconsultables respectent la LPRP et ses propres politiques. Le CPVP effectuera une vérification a posteriori.

Le rapport de vérification complet se trouve sur le site Web du Commissariat.

Projet Shock

Le fichier inconsultable des dossiers d'enquêtes relatives à la sécurité nationale de la GRC comprend des dossiers liés au « Projet Shock », initiative pour la coordination des indices reçus concernant les attaques terroristes du 11 septembre 2001.

Le Commissariat a examiné un échantillon des dossiers en 2002 et a trouvé que les indices portaient généralement sur des soupçons d'affiliation terroriste, des personnes louches ou des activités suspectes. Cependant, certains indices tenaient plutôt de l'hystérie collective en période de crise.

Bien que ces fichiers ne fassent pas partie de la vérification des fichiers inconsultables, le CPVP a posé des questions pour vérifier si chaque dossier d'indice avait été évalué en fonction de la pertinence de le conserver parmi les fichiers inconsultables.

Tel que nous l'avons indiqué dans notre rapport spécial, un examen ultérieur par la GRC des dossiers du « Projet Shock », contenant des renseignements sur des milliers de citoyens, a révélé que ces dossiers étaient non-conformes au critère d'inclusion continue dans le fichier inconsultable relatif à la sécurité nationale et ils en ont donc été retirés.

Le travail de vérification du CPVP a donné lieu cette année à notre premier rapport spécial au Parlement. Les problèmes découverts pendant une vérification des fichiers inconsultables de la GRC ont suscité de si grandes inquiétudes que la commissaire a choisi d'en produire les conclusions dans un rapport spécial présenté en février 2008. Le Commissariat a également réalisé un examen complet des activités de Passeport Canada (voir page 17).

La Direction de la vérification et de la revue s'est penchée sur d'autres questions au cours de 2007-2008, dont l'achat par le gouvernement de renseignements personnels à des courtiers en données et l'utilisation répandue du numéro d'assurance sociale. Le CPVP a aussi étudié les évaluations des facteurs relatifs à la vie privée (ÉFVP) de nouvelles initiatives fédérales, ce qui nous a permis de faire des centaines de recommandations visant à protéger la vie privée des Canadiennes et des Canadiens.

Rapport spécial au Parlement concernant les fichiers inconsultables de la GRC

Une vérification du Commissariat a permis de découvrir que les fichiers inconsultables de la GRC, qui soustraient à l'accès du public des dossiers sur la sécurité nationale et des renseignements criminels, avaient été truffés de dizaines de milliers de dossiers qui n'auraient pas dû s'y trouver. Cette conclusion est particulièrement troublante, car la GRC avait déjà été avisée 20 ans plus tôt de problèmes de conformité à ce sujet et s'était engagée à tenir convenablement ces fichiers.

Les fichiers inconsultables servent à cacher les renseignements les plus délicats sur la sécurité nationale et la criminalité. Les ministères et les organismes qui contrôlent de tels fichiers refuseront de confirmer ou nieront l'existence de tels renseignements en cas de demande d'accès.

autres personnes mentionnées malgré qu'elles ne soient pas nommées, mais il estimait que l'intérêt public l'emportait sur le droit à la vie privée.

Le Bureau de l'Ombudsman a avisé quatre personnes de la publication imminente du rapport et leur a remis le document. Le CPVP a étudié la question et a recommandé que soient informées les deux autres personnes de la publication du rapport et du risque qu'elles soient identifiées. Cette recommandation a été acceptée.

Un rapport de la Commission d'examen des plaintes révèle des renseignements personnels

La Commission d'examen des plaintes concernant la police militaire est un organisme fédéral indépendant chargé de surveiller le traitement des plaintes relatives à la conduite des membres de la police militaire.

La Commission d'examen des plaintes a reçu une plainte d'un tireur d'élite provenant d'une unité déployée en Afghanistan au sujet de la conduite de membres de la police militaire. La Commission a enquêté sur les allégations et a avisé le CPVP de son intention de communiquer des renseignements personnels contenus dans son rapport en le publiant sur son site Web. La Commission d'examen des plaintes a fait valoir que le rapport contenait des informations d'intérêt public cruciales.

La Commission a déterminé que les allégations qui visaient la police militaire n'étaient pas fondées.

Les plaignants, les membres de la police militaire, le ministre de la Défense nationale ainsi que d'autres fonctionnaires ministériels ont eu le rapport avant sa publication sur Internet et ont été informés qu'il serait rendu public. D'autres personnes nommées dans le rapport parce qu'elles avaient été interrogées au cours de l'enquête n'ont pas été avisées. Le CPVP a recommandé à la Commission d'aviser les personnes interrogées de son intention de publier le rapport. Il a également recommandé sa dépersonnalisation afin de protéger l'identité des parties et des personnes interrogées.

Autres exemples de communications pour raisons d'intérêt public

Un risque de transmission de la tuberculose oblige l'identification d'un passager

Le ministre des Affaires étrangères et du Commerce international a informé le CPVP qu'il avait communiqué à l'Agence de la santé publique du Canada l'identité et les coordonnées de 27 passagers sur un vol international de plus de huit heures dont les sièges étaient à proximité de celui d'une personne ayant la tuberculose.

L'Agence de la santé publique a pu ainsi informer les passagers concernés de la nécessité de subir un test de dépistage de la tuberculose.

Dans cette affaire, des raisons d'intérêt public l'emportaient nettement sur toute possible atteinte à la vie privée.

La vérificatrice générale met au jour l'emploi inapproprié de fonds par la lieutenant-gouverneure du Québec

Le Bureau du vérificateur général du Canada a informé le CPVP de son intention de communiquer des renseignements personnels liés à l'utilisation inappropriée de fonds fédéraux par la lieutenant-gouverneure du Québec.

La vérificatrice générale a étayé sa décision de communiquer des renseignements personnels par des raisons d'intérêt public. Le Commissariat a conclu qu'aucune autre mesure n'était nécessaire.

L'ombudsman de la Défense nationale publie un rapport sur des tireurs d'élite des Forces canadiennes

Le Bureau de l'Ombudsman de la Défense nationale et des Forces canadiennes a informé le CPVP de son intention de publier le rapport intitulé : *La bataille d'un tireur d'élite : l'incapacité d'un père – Une enquête sur le traitement d'un tireur d'élite des Forces canadiennes déployé en Afghanistan en 2002 – Rapport spécial à l'intention du ministre de la Défense nationale et du Chef d'état-major de la Défense.*

Le rapport concerne les allégations faites par le père d'un des six tireurs d'élite d'une unité. Il affirmait que les hommes avaient été ostracisés et traités de façon injuste, qu'on leur avait refusé le droit aux séances de verbalisation et qu'on les avait soumis, sans justification, à des enquêtes criminelles et à d'autres types de enquêtes.

Deux personnes nommées dans le rapport ont consenti à la communication de leurs renseignements personnels. L'ombudsman était d'avis qu'il était possible d'identifier les

quantité de chèques imprimés est comparée au nombre d'enveloppes à poster. Tout écart conduit immédiatement à une vérification et à une correction. De plus, l'entreprise a mis en place une politique qui oblige dorénavant l'insertion individuelle des chèques de remboursement.

Anciens Combattants Canada a appelé les prestataires concernés pour vérifier s'ils avaient bien reçu leur chèque et l'entreprise a envoyé une lettre d'excuses. Les chèques ont été soit réacheminés au bon destinataire soit réémis.

Le Commissariat a examiné le rapport du ministère des Anciens Combattants sur cet incident et est satisfait des mesures prises pour aviser les personnes touchées et pour s'assurer qu'une telle situation ne se reproduise pas.

Communications pour raisons d'intérêt public en vertu de la LPRP

Quand l'intérêt public l'emporte nettement sur le droit à la vie privée d'une personne, le responsable d'une institution fédérale peut, en vertu de la LPRP, utiliser son pouvoir discrétionnaire et communiquer des renseignements personnels sans consentement.

À moins qu'il ne s'agisse d'une urgence, l'institution qui communique des renseignements personnels dans l'intérêt du public doit prévenir la commissaire à la protection de la vie privée. Après examen des renseignements en question, la commissaire peut, si elle le juge nécessaire, aviser la personne concernée que des renseignements la concernant seront communiqués. Le CPVP indiquera également des façons de limiter la quantité de renseignements personnels à communiquer s'il juge que la proposition de l'institution excède ce qui satisfait aux questions d'intérêt public.

En 2007-2008, le Commissariat a examiné 83 avis de communication pour raison d'intérêt public. La plupart provenaient de la GRC et concernaient des délinquants à risque élevé qui allaient être mis en liberté et qui, selon l'institution, représentaient une menace pour la collectivité. Dans d'autres cas, la GRC a communiqué des renseignements personnels pour retracer un suspect ou pour mettre en garde le public contre les comportements d'un délinquant violent ou d'un délinquant sexuel.

D'autres avis de communication de la Défense nationale et du Service correctionnel du Canada visaient à informer les membres d'une famille du décès d'un des leurs. Ce type de renseignements sur la cause d'un décès est fourni pour des raisons de compassion.

L'employé a immédiatement prévenu la police du vol. Des fonctionnaires de Statistique Canada ont rencontré chacun des ménages concernés pour les informer que leurs renseignements personnels avaient été compromis.

Statistique Canada a abordé le problème de manière appropriée avec l'employé victime du vol. Le ministère a aussi envoyé un bulletin d'information à tous les employés sur le terrain pour leur rappeler leur obligation de protéger leur portable et de contrôler l'utilisation des mots de passe, du nom d'utilisateur et des comptes. Le Commissariat est satisfait des mesures mises en œuvre par Statistique Canada.

Une erreur humaine compromet les renseignements personnels de contribuables

Une personne ayant utilisé le service téléphonique de l'Agence du revenu du Canada (ARC) pour obtenir de l'information sur son régime enregistré d'épargne-retraite a reçu une enveloppe renfermant les avis de cotisation de neuf autres contribuables.

Le citoyen a téléphoné à l'ARC pour rapporter la situation, mais la communication avec l'agent qui lui a répondu s'est avérée ardue. Il a demandé à parler à un superviseur, ce qui lui a d'abord été refusé. Un superviseur a ensuite communiqué avec le citoyen pour lui demander de retourner les documents. Ayant eu l'impression que l'ARC ne prenait pas l'affaire au sérieux, le citoyen a communiqué avec deux chaînes de télévision.

Des équipes de tournage ont filmé le citoyen alors qu'il livrait un avis de cotisation à une personne qui habitait à proximité, puis retournait les autres documents à un bureau de l'ARC.

Après l'incident, l'Agence du revenu du Canada a révisé ses procédures et ses politiques sur les documents à télécopier ou à poster et a apporté des correctifs. L'ARC a également présenté ses excuses aux contribuables concernés.

Le Commissariat a conclu que l'incident résultait d'une erreur humaine.

Une machine à mettre sous pli qui n'avait pas été réinitialisée cause une atteinte à la vie privée

Un employé d'une société privée chargée de l'administration du Programme pour l'autonomie des anciens combattants d'Anciens Combattants Canada a oublié de réinitialiser une machine à mettre sous pli, causant ainsi l'insertion de deux chèques dans une même enveloppe, et ce, pour 122 chèques (insérés dans 61 enveloppes).

L'entreprise a fait enquête et a mis en place un nouveau système d'assurance de la qualité. Ainsi, le nombre de chèques traités dans une journée est maintenant consigné, puis la

Le destinataire d'un des CD contenant l'information demandée en format PDF a informé TPSGC qu'il arrivait à lire les renseignements qui avaient été retirés. Il a dit n'avoir eu qu'à copier les parties dépersonnalisées dans un autre document.

Avant d'avoir vent de ce problème, TPSGC avait répondu à 123 demandes en vertu de la *Loi sur l'accès à l'information* et à une demande en vertu de la LPRP au moyen de fichiers PDF. En conséquence, le contenu des CD envoyés pouvait révéler le nom et l'adresse de résidence d'employés fédéraux faisant l'objet d'une enquête relative à une fraude impliquant des cartes de crédit de l'administration fédérale, le nom et la date de naissance de personnes en attente d'une cote de sécurité, le résultat d'évaluations de langue seconde et des renseignements sur les congés.

Afin de limiter toute autre communication induite de renseignements, TPSGC a tenté de récupérer les CD. Certains les ont retournés, alors que d'autres ont affirmé les avoir détruits ou perdus. Les personnes dont les renseignements personnels étaient menacés ont été avisées par l'organisme du risque d'atteinte à leur vie privée.

Il a été établi que le problème venait d'une défaillance du système de numérisation. TPSGC a contacté le fournisseur du logiciel, qui a affirmé que TPSGC était la seule institution à avoir une version défectueuse. Malgré tout, afin d'éviter que la situation ne se reproduise ailleurs, le Conseil du Trésor a préparé un bulletin de sécurité avisant l'ensemble des institutions de ne pas communiquer de renseignements sur CD jusqu'à ce qu'elles aient la confirmation que leur logiciel est sécuritaire.

Un portable vole contient des renseignements d'enquête auprès des ménages

Un ordinateur portable volé au domicile d'un employé de Statistique Canada contenait des renseignements personnels chiffrés sur plusieurs citoyens qui avaient répondu à des sondages. Malheureusement, l'employé avait noté les deux mots de passe nécessaires pour avoir accès aux données sur un bout de papier rangé dans la mallette de l'ordinateur.

L'ordinateur contenait les données de six enquêtes sur la population active et sur la santé dans les collectivités canadiennes. Les données sur la population active comportaient des coordonnées et des renseignements sur le ménage, le loyer, l'emploi et les revenus ainsi que des données démographiques, tandis que celles des enquêtes sur la santé comportaient des renseignements extrêmement confidentiels, y compris la taille, le poids, les habitudes de sommeil, les comportements sexuels, les maladies chroniques, le niveau de stress, l'usage du tabac, la consommation d'alcool et de drogues ainsi que l'état de santé mentale.

Atteintes à la sécurité des données

Le Secrétaire du Conseil du Trésor a publié à la fin de mars 2007 des lignes directrices sur les atteintes à la vie privée à l'intention des institutions assujetties à la LPRP. Ces lignes directrices « recommandent fortement » aux institutions fédérales d'aviser le CPVP si une atteinte à la sécurité porte sur des renseignements personnels de nature délicate, comme des renseignements de nature financière ou médicale ou des numéros d'assurance sociale, ou s'il y a risque de vol d'identité, de préjudice ou d'humiliation menaçant la réputation, la situation financière ou la sécurité d'une personne.

La première année de la mise en place de ces lignes directrices, le Commissariat a remarqué une augmentation du nombre d'incidents qui lui sont signalés (57 en 2007-2008 contre 43 en 2006-2007). La quantité de renseignements personnels détenue par les institutions fédérales étant impressionnante, ce relativement petit nombre d'incidents est plutôt encourageant.

La plupart des incidents résultaient d'une erreur humaine ou d'un vol, comme lorsque des documents contenant des renseignements personnels sur une personne ont été perdus, lorsqu'un porte-documents appartenant à un fonctionnaire a été volé dans une chambre d'hôtel ou lorsqu'un portable a été volé dans un véhicule. Dans un des cas, des employés ont obtenu un accès non autorisé à des renseignements personnels conservés sur des ordinateurs du gouvernement.

Voici quelques incidents types que nous avons examinés :

Un problème technique mène à la communication de renseignements de nature délicate

En faisant parvenir les réponses à des demandes en vertu de la Loi sur l'accès à l'information sur des CD plutôt que sur des documents papier, Travaux publics et Services gouvernementaux Canada (TPSGC) a fait une tentative infructueuse de retirer des renseignements confidentiels, ce qui a compromis les renseignements personnels de nombreuses personnes.

Ces dernières années, des institutions ont pris l'habitude de répondre à certaines demandes en vertu de la Loi sur l'accès à l'information et de la LPRP sur CD au lieu d'utiliser du papier. À TPSCG, les CD contenaient des reproductions numérisées en format TIFF (Tagged Image File Format) des documents. Lorsque des personnes se sont plaintes d'éprouver des difficultés à ouvrir ces fichiers, le format d'enregistrement a été changé pour le format PDF (Portable Document Format).

Communication injustifiée de renseignements à un employeur potentiel

Un homme a affirmé que Ressources humaines et Développement des compétences (RHDCC, maintenant Service Canada) avait communiqué de façon injustifiée son numéro d'assurance sociale, son adresse, sa date de naissance, des renseignements sur ses revenus et des données concernant sa demande d'assurance-emploi à un employeur potentiel.

Le plaignant avait refusé une offre d'emploi pendant une période où il bénéficiait de prestations d'assurance-emploi (AE), en conséquence de quoi, RHDCC a mis fin à ses prestations d'AE. Le plaignant a interjeté appel de cette décision devant le conseil arbitral, car il a indiqué qu'il avait refusé l'emploi en raison des conditions de travail.

Conformément à la *Loi sur l'assurance-emploi*, lorsqu'une personne interjette appel

devant le conseil arbitral, RHDCC peut communiquer des renseignements sur la personne aux parties intéressées, comme des employeurs ou toute personne ayant un intérêt direct. La communication de renseignements à ces parties est nécessaire pour établir la validité de la demande de rétablissement des prestations d'AE.

Dans cette affaire, RHDCC a jugé que l'employeur potentiel était une partie dans l'appel du plaignant. RHDCC a donné à l'entreprise une foule de renseignements sans avoir relu le dossier du plaignant, et de ce fait a communiqué le numéro d'assurance sociale, la date de naissance et des renseignements sur les emplois précédents, y compris les taux de rémunération régulière et majorée. Comme l'appel devant le conseil arbitral était fondé sur le refus d'un emploi en raison des conditions de travail, les renseignements communiqués par RHDCC auraient dû se limiter à ce qui était nécessaire pour valider la décision du plaignant de refuser l'offre d'emploi.

RHDCC a reconnu avoir communiqué trop de renseignements et a parlé de l'incident comme d'une erreur involontaire commise en toute bonne foi par un employé. À la suite de cette plainte, l'organisme a révisé ses politiques et ses procédures, puis a changé la définition d'employeur pour ce qui suit : une personne ou un organisme pour lequel le requérant travaille ou a déjà travaillé. Un futur employeur ou un employeur potentiel n'est plus considéré comme une partie intéressée dans le processus d'appel.

La plainte était fondée.

Incidents en vertu de la LPPR

Le Commissariat examine aussi des cas de mauvaise gestion des renseignements personnels qui sont portés à son attention par les médias, par des personnes touchées ou par un avis d'atteinte à la sécurité des données émis par une institution fédérale.

Le courriel avait été rédigé après une conférence téléphonique entre plusieurs ministères durant laquelle un fonctionnaire de Sécurité publique Canada avait discuté de la communication prochaine d'information concernant une question de nature délicate en réponse à une demande faite en vertu de la *Loi sur l'accès à l'information*. Dans le courriel, le fonctionnaire du BCP mentionnait la possibilité que le plaignant rédige un nouvel article concernant une affaire délicate qu'il avait déjà traitée. D'autres journalistes étaient également nommés dans le courriel, principalement en ce qui a trait à des articles déjà publiés. Les noms avaient été masqués, mais celui du plaignant avait été oublié et communiqué par erreur.

Le Bureau du Conseil privé a par la suite présenté ses excuses au plaignant. Comme le nom du plaignant avait été communiqué à l'autre journaliste en réponse à une demande faite en vertu de la *Loi sur l'accès à l'information*, le CPVP a conclu qu'il y avait eu atteinte au droit à la vie privée du plaignant. La plainte était fondée.

Une plainte connexe comportait des allégations voulant que le fonctionnaire du BCP ait communiqué le fait que le journaliste avait présenté une demande d'accès à l'information à Sécurité publique Canada lors de la conférence téléphonique entre plusieurs ministères. Toutefois, notre enquête a confirmé que l'identité de la personne ayant fait la demande d'accès à l'information n'avait jamais été communiquée à l'extérieur du bureau d'AIPRP de Sécurité publique Canada.

Le fonctionnaire du BCP a déclaré qu'il avait uniquement émis une hypothèse à propos de l'auteur de la demande en fonction du fait que le journaliste avait rédigé plusieurs articles sur le sujet.

Le commissaire adjoint s'est dit convaincu que l'identité du journaliste en tant qu'auteur de la demande d'accès à l'information n'avait pas été communiquée au BCP et n'était donc pas de la responsabilité du BCP. Cette plainte était non fondée.

Une troisième plainte émanant du même journaliste, dans laquelle celui-ci alléguait que Sécurité publique Canada l'avait identifié comme l'auteur d'une demande d'accès à l'information était également non fondée. Le dossier de plainte a été fermé l'année dernière.

Plus tard, l'employé a reçu une copie du mandat pour l'enquête administrative et a remarqué l'absence de signature. Il a allégué que, le document n'étant pas signé, le Ministère n'avait pas l'autorité de reconstituer ou de lire les courriels. Il a également prétendu qu'il aurait dû être avisé des mesures prises par l'institution.

La politique du Conseil du Trésor en la matière précise que si une institution a des raisons valables de soupçonner une personne d'utiliser le réseau à mauvais escient, elle doit faire part de ses soupçons au dirigeant qui est responsable d'enquêter et de prendre des mesures de contrôle particulières, ce qui peut comprendre la lecture du contenu des courriels de la personne.

La politique du ministère des Affaires indiennes et du Nord canadien prévoit que la direction peut avoir accès aux courriels d'un employé dans le cadre d'une enquête sur des pratiques répérhensibles, des atteintes à la sécurité et des infractions à la loi ou aux politiques du Ministère.

Bien que le mandat n'ait pas été signé et que l'employé n'ait pas été informé des mesures prises par son employeur, le Ministère n'a pas violé la Politique du Conseil du trésor sur l'utilisation des réseaux électroniques, ni le droit à la vie privée de l'employé. En vertu de la LPRP, les renseignements personnels relevant d'une institution fédérale ne peuvent servir qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins. Dans cette affaire, les renseignements recueillis à partir des courriels du plaignant n'ont servi qu'aux fins de l'enquête administrative du Ministère.

La plainte était non fondée.

Un journaliste est identifié dans une réponse à une demande d'accès

Un journaliste s'est plaint que son nom avait été communiqué de façon indue dans une réponse à une demande faite en vertu de la Loi sur l'accès à l'information. Le nom du journaliste apparaissait dans un courriel rédigé par un employé du Bureau du Conseil privé.

Le courriel a été mis au jour après qu'un autre journaliste a fait une demande d'accès à l'ensemble des courriels et des communications que le directeur des communications du Cabinet du Premier ministre avait envoyés ou reçus.

La réponse à cette demande comprenait un courriel qu'un employé du Bureau du Conseil privé (BCP) avait adressé à 19 responsables gouvernementaux du BCP et du Cabinet du Premier ministre.

membres. Le plaignant avait fait une demande en vertu de la LPRP pour connaître les renseignements personnels que détenaient cinq de ses collègues, aussi membres du syndicat, et les auteurs des critiques à son égard.

À la suite de la demande faite au MAECI, le service de l'AIPRP a demandé aux collègues de fournir tous les renseignements personnels qu'ils détenaient sur le plaignant. Le personnel de l'AIPRP a avisé les collègues de la confidentialité de la demande et les a informés que la diffusion de ces renseignements au sein du MAECI devait respecter le principe du « besoin de connaître ».

Le Commissariat a d'abord étudié la crainte du plaignant d'être identifié comme l'auteur de la demande. La plainte était non fondée, car pour obtenir les renseignements que détenaient les collègues, le service de l'AIPRP devait communiquer l'identité du plaignant.

Quant à la préoccupation du plaignant concernant le fait que les collègues avaient avisé le syndicat de la demande faite en vertu de la LPRP, l'enquête du Commissariat a permis de confirmer que quatre des cinq collègues avaient informé l'Alliance de la Fonction publique du Canada des gestes du plaignant. Les collègues ont cru que le plaignant avait fait la demande dans le but de les harceler. Les quatre collègues concernés ont confirmé avoir lu le rappel sur la confidentialité de la demande, mais ils ont indiqué avoir considéré la question comme une affaire syndicale et non ministérielle.

Si la communication de l'identité du plaignant à ses collègues était une plainte non fondée, le fait que quatre collègues ont informé le syndicat de la demande du plaignant en vertu de la LPRP constituait une atteinte au droit à la vie privée.

La plainte était fondée.

La surveillance des courriels d'un employé se révèle appropriée

Un employé du ministère des Affaires indiennes et du Nord canadien s'est plaint du fait que son employeur n'avait pas l'autorité de reconstituer ses courriels sur 35 mois et de relire tous les messages de son compte au Ministère. L'employé a prétendu que les gestes posés par son employeur constituaient un accès injustifié à ses renseignements personnels.

L'employé faisait l'objet d'une enquête administrative à la suite d'allégations selon lesquelles il utilisait le réseau du ministère à mauvais escient.

Pendant l'enquête sur les gestes du plaignant, le Ministère a reconstitué le compte de courriel du plaignant et y a découvert des messages au contenu pornographique.

Afin de s'assurer que la situation ne se reproduise plus, le Service correctionnel du Canada a ordonné à l'établissement de cesser l'affichage de ce genre de renseignements dans le bureau à proximité d'un lieu fréquenté par des détenus et d'être plus vigilant à l'égard des renseignements personnels.

La plainte était fondée.

Une employée de l'Agence du revenu du Canada fait un usage abusif de renseignements

Une femme s'est plainte que son ancienne voisine, qui travaillait pour l'Agence du revenu du Canada (ARC), avait obtenu accès à son dossier d'impôt de façon abusive pour connaître son lieu de travail, puis avait utilisé l'information pour la harceler au téléphone et lui faire des menaces.

La plaignante n'en était pas à ses premiers démêlés avec l'employée de l'ARC. Elle a déclaré que l'employée et sa famille la harcelaient et la menaçaient depuis des années. La plaignante a déménagé et a obtenu un numéro de téléphone confidentiel. Après son déménagement, elle a commencé à se faire harceler par téléphone au travail et elle a établi que les appels provenaient de l'employée en question.

L'Agence a confirmé que son employée s'était servie de son poste pour avoir accès aux renseignements personnels de la plaignante, c'est-à-dire son adresse, son numéro d'assurance sociale, son lieu de travail, son revenu et ses déductions fiscales. L'ARC a mis l'employée en présence des faits et l'employée a confirmé qu'elle avait consulté les renseignements fiscaux de la plaignante. L'employée a fait l'objet de mesures disciplinaires pour avoir consulté sans autorisation les renseignements personnels de la plaignante.

L'ARC dispose d'un processus de vérification des accès élaboré qui lui permet de protéger les renseignements des contribuables.

La plainte était fondée.

L'identité de l'auteur d'une demande de renseignements est révélée

Un employé s'est plaint du fait que son employeur, le ministère des Affaires étrangères et du Commerce international (MAECI), avait communiqué sans justification ses renseignements personnels à des collègues, qui les avaient ensuite communiqués à l'Alliance de la Fonction publique du Canada.

En plus d'être un employé du MAECI, le plaignant avait fait l'objet de critiques en ce qui concerne son travail syndical de la part des dirigeants locaux et de quelques

Plaintes – Exemples de cas ayant fait l'objet d'une enquête du CPVP

Passeport Canada présente ses excuses pour avoir fait une « erreur inacceptable »

Le plaignant a posté sa demande de renouvellement de passeport à Passeport Canada. Comme exigé, il a inclus dans l'envoi son passeport venant à échéance, des photocopies de son permis de conduire et de sa carte d'assurance maladie, ainsi que l'original de son acte de naissance. Lorsqu'il a reçu son nouveau passeport, l'enveloppe contenait également le passeport échu et les documents personnels d'une autre personne.

Le plaignant a signalé l'erreur à Passeport Canada, qui lui a demandé de retourner les documents ne lui appartenant pas – ce qu'il a fait – et a indiqué qu'il chercherait les documents du plaignant. Passeport Canada a communiqué avec l'autre personne, qui a indiqué avoir détruit les documents du plaignant.

Notre enquête a permis de déterminer qu'un employé de Passeport Canada avait interverti le contenu des dossiers, puis avait négligé de s'assurer que les enveloppes, les nouveaux passeports et les autres documents correspondaient bien à chacun des destinataires.

Passeport Canada a présenté ses excuses pour ce qu'il a reconnu être une « erreur inacceptable » et il a indiqué avoir pris des mesures pour que la situation ne se reproduise pas. Les cadres tiennent maintenant des réunions mensuelles avec le personnel pour s'assurer que les procédures adéquates sont bien suivies. De plus, l'organisme affiche les procédures et les nouveaux employés reçoivent une formation qui souligne l'importance de vérifier les documents avant de les insérer dans une enveloppe et de les poster au destinataire.

La plainte était fondée.

Un rapport concernant des détenus est trouvé dans une poubelle du gymnase d'une prison

Un rapport comportant des photos, le nom, la date de naissance, le numéro de cellule de 96 détenus, ainsi que d'autres renseignements personnels, a été découvert dans la cellule d'un détenu en Alberta. Quatorze des détenus concernés ont porté plainte au CPVP.

Un détenu a découvert le rapport dans une poubelle du gymnase de la prison. L'enquête du Service correctionnel du Canada a permis de déterminer que ce rapport était régulièrement mis à jour et affiché pour les agents de correction dans un bureau à proximité du gymnase. Les rapports périmés étaient régulièrement jetés dans la poubelle du gymnase.

Un autre défi de taille consiste à attirer et à retenir des enquêteurs expérimentés et des gestionnaires dans ce domaine. Les personnes qui connaissent bien l'application de la LPRP et qui ont de l'expérience en enquête sont en grande demande dans la fonction publique — il n'y a tout simplement pas assez de personnes compétentes pour répondre aux besoins. Une génération plus âgée prend sa retraite et la nouvelle génération est extrêmement mobile dans un marché de l'emploi compétitif. Le taux de roulement du personnel dans ce domaine a été plus élevé qu'ailleurs au CPVP en raison de départs à la retraite et d'une demande externe.

Le Commissariat continue le renouvellement de son service d'enquête en misant sur le recrutement et en cherchant des façons novatrices d'améliorer ses services.

La stratégie comporte une réingénierie du processus d'enquête qui simplifiera les demandes de renseignements, les plaintes et les enquêtes. Les plaintes seront triées et nous déterminerons lesquelles sont susceptibles de se régler rapidement. Un nouveau système de gestion des dossiers permettra de mieux cerner les tendances et de concentrer les ressources là où elles seront le plus efficace.

Le Commissariat prévoit qu'une année sera nécessaire pour renforcer les capacités, diminuer les plaintes en attente et continuer l'embauche et la formation de personnel additionnel pour enquêter de façons novatrices. L'objectif est de terminer la réingénierie au printemps 2009.

Formation et coopération intergouvernementale

La formation jouera un grand rôle dans les efforts constants du Commissariat pour améliorer les méthodes d'enquête et de résolution des plaintes relatives aux atteintes à la vie privée.

En février 2008, le CPVP a tenu la quatrième conférence annuelle des enquêteurs. Plus de 90 personnes ont participé à cette conférence tenue à Ottawa, y compris des représentants de 12 des 13 organismes chargés de la protection de la vie privée dans les provinces et les territoires, et pour la première fois, des membres du Commissariat à l'information du Canada. La conférence a permis aux enquêteurs d'échanger sur leurs expériences et sur les meilleures pratiques. Des débats francs et ouverts ont amélioré la connaissance des enjeux communs.

Accès aux renseignements personnels

Le droit d'accès aux renseignements personnels détenus par une institution fédérale est un droit fondamental que la LPRP accorde aux personnes. Toutefois, de toute évidence, beaucoup de citoyens éprouvent des difficultés à exercer ce droit. Plus de 70 p. 100 des plaintes déposées au Commissariat le sont par des personnes préoccupées par le refus d'accès à leurs renseignements personnels ou par l'incapacité d'une institution à communiquer ces renseignements dans les délais prescrits.

Le CPVP se réjouit de constater que les plaintes de ce genre ont diminué au cours des dernières années. La diminution peut être attribuable au fait que les personnes traitent directement avec les institutions pour régler les situations, une pratique encouragée par le Commissariat.

Un dossier de plainte liée au délai de réponse est ouvert lorsqu'une personne avise le Commissariat qu'une institution n'a pu répondre à la demande dans les 30 jours, comme le stipule la Loi. Dans certains dossiers, une année s'est écoulée sans que les institutions aient répondu aux demandes. Un plaignant a même attendu plus de deux ans une réponse à sa demande.

Défis que posent les enquêtes et demandes de renseignements

Le CPVP a ses propres défis à relever quand il s'agit de répondre rapidement aux plaintes et il est fermement déterminé à réduire le délai de traitement des plaintes. En 2007-2008, le CPVP a reçu 759 plaintes et fermé 880 dossiers de plainte. Le CPVP avait 370 plaintes en attente de traitement qui, faute d'enquêteurs, n'étaient pas assignées. En moyenne, les enquêtes ont été menées à terme en 14,5 mois. Nous savons que cette situation est inacceptable et nous prenons certaines mesures pour remédier à la situation. Vous trouverez une répartition détaillée des délais de traitement par conclusion et par type de plainte à l'annexe 3.

Le Commissariat se heurte à l'obligation, en vertu du libellé de la LPRP, de traiter chacune des plaintes qu'il reçoit. D'autres autorités de protection des données des quatre coins du monde et des provinces canadiennes sont aussi confrontées à l'obligation d'examiner toutes les plaintes déposées, peu importe leur nature ou leur gravité. Le CPVP a demandé au gouvernement de modifier les lois afin d'obtenir la souplesse qui lui permettrait d'arriver à une meilleure utilisation de ses ressources d'enquête (pour de plus amples renseignements, voir page 50).

La plupart des nouvelles plaintes provenaient de personnes qui alléguaient que des institutions fédérales leur avaient refusé le droit d'accès à leurs renseignements personnels. Le deuxième type de plainte en nombre porte sur la limite de 30 jours (pouvant être prolongée jusqu'à 60 jours dans certains cas) fixée par la loi pour répondre à une demande d'accès.

Vous trouverez des renseignements détaillés sur les plaintes reçues par type à l'annexe 3.

Plaintes fermées en 2007-2008	
Total	880

Les trois principales catégories de plaintes fermées	
Refus d'accès	318
Non-respect du délai	301
Utilisation/communication inappropriée	134
de renseignements personnels	

Répartition des plaintes fermées	
Abandonnées	117
Réglées rapidement	32
Réglées en cours d'enquête	114
Résolues	6
Non fondées	275
Fondées	319
Fondées et résolues	17
Total	880

Les personnes peuvent abandonner leur plainte lorsque le problème a été résolu avec l'institution avant le début de l'enquête. Le CPVP peut également abandonner la plainte s'il manque des renseignements nécessaires pour terminer l'enquête. Une plainte réglée rapidement ou réglée en cours d'enquête indique que la personne est satisfaite des mesures prises par l'institution à la suite de l'intervention du Commissariat.

Demandes de renseignements

En 2007-2008, le Commissariat a reçu 4 258 demandes de renseignements en vertu de la LPRP en plus de 2 367 demandes plus générales sur la protection de la vie privée. Ces chiffres s'ajoutent aux 7 636 demandes de renseignements sur la LPRPDE, la loi applicable au secteur privé, reçues en 2007. Le nombre moyen de demandes reçues chaque jour au sujet de toutes les questions de protection de la vie privée est de près de 60.

Notre unité de demandes de renseignements fournit un service très important aux Canadiennes et aux Canadiens, qui peuvent obtenir une réponse en temps opportun à des questions concernant un vaste éventail d'enjeux liés à la protection de la vie privée.

Plaintes

Le CPVP a reçu 759 nouvelles plaintes, un peu moins que les 839 de l'année précédente. La quantité de plaintes déposées contre les institutions ne signifie pas nécessairement que celles-ci ne respectent pas la LPRP.

En raison de leur mandat, certaines institutions détiennent une quantité considérable de renseignements personnels et sont donc plus susceptibles de recevoir de nombreuses demandes d'accès aux renseignements. Ainsi, les probabilités sont plus grandes qu'elles fassent l'objet de plaintes relatives à la collecte, à l'utilisation, à la communication, à la conservation et au retrait de renseignements personnels ou à la façon dont elles donnent accès aux renseignements.

Depuis quelques années, les institutions qui ont fait l'objet du plus grand nombre de plaintes sont le Service correctionnel du Canada et la GRC. Il convient de noter que les plaintes contre la GRC diminuent constamment, tandis que celles contre le Service correctionnel du Canada ont considérablement augmenté – de 190 en 2005-2006 à 248 en 2007-2008. Cette hausse du nombre de plaintes contre le Service correctionnel du Canada pourrait être directement proportionnelle à la hausse des demandes d'accès aux renseignements personnels que connaît ce service.

Vous trouverez une liste complète des plaintes reçues par institution à l'annexe 3.

De plus, le Commissariat est encore préoccupé par la question des retards dans le traitement des demandes des citoyens concernant l'accès à leurs renseignements personnels. Si certains ministères ont amélioré les délais de réponse, beaucoup des sections de l'accès à l'information et de la protection des renseignements personnels (AIPRP) sont débordées.

NOTE : Les annexes comportent des tableaux statistiques détaillés, les définitions de chaque type de plaintes et de conclusions ainsi qu'une description du processus d'enquête dans le cadre de la LPRP.

Coup d'œil sur les demandes de renseignement, les plaintes et les enquêtes

Demandes de renseignements

Demandes de renseignements en vertu de la LPRP reçues 4 258
Demandes de renseignements sur la protection de la vie privée en général 2 367
Total (sans les demandes de renseignements en vertu de la LPRPE) 6 625

Plaintes

Nombre total de nouvelles plaintes reçues 759

Les 10 institutions ayant reçu le plus de plaintes

Service correctionnel du Canada	248
Gendarmerie royale du Canada	84
Agence des services frontaliers du Canada	54
Service Canada	52
Défense nationale	48
Service canadien du renseignement de sécurité	45
Agence du revenu du Canada	38
Société canadienne des postes	28
Affaires étrangères et Commerce international	27
Justice Canada	18
Autres	117
Total	759

RÉPONSE AUX PLAINTES ET AUX INCIDENTS RELATIFS À LA PROTECTION DE LA VIE PRIVÉE

Aperçu de la façon dont le CPVP a traité les plaintes et les incidents dans le cadre de la Loi sur la protection des renseignements personnels (LPPRP) en 2007-2008.

Les plaintes reçues montrent que les Canadiennes et les Canadiens ont un large éventail de préoccupations quant à la façon dont les institutions fédérales traitent leurs renseignements personnels.

Les citoyens sont inquiets des échanges de renseignements entre les ministères, de l'utilisation du courriel pour consigner ou communiquer des renseignements ainsi que des problèmes que pose le fait pour les institutions de conserver des renseignements personnels dans des ordinateurs et d'accorder de façon opportune les droits d'accès aux renseignements personnels.

Le Commissariat a également remarqué une préoccupation grandissante quant à la manière dont les institutions fédérales protègent les renseignements. Les grands titres annonçant que des renseignements personnels ont été égarés ou volés alors que des fonctionnaires travaillaient à distance ou qu'ils avaient apporté le portable du bureau pour travailler à la maison n'ont rien pour inspirer confiance au public.

Les affaires qui ont fait l'objet d'une enquête du CPVP cette année ont mis en lumière à quel point une erreur humaine peut mettre à risque la vie privée. Certaines des atteintes que nous avons étudiées illustrent comment les problèmes d'ordinateurs et d'utilisation de l'équipement électronique conçu pour améliorer les processus administratifs peuvent mener à la communication de renseignements personnels. Il est également clair que les institutions fédérales doivent continuer d'insister auprès de leur personnel sur l'importance de la protection des renseignements personnels et de la vie privée.

L'objectif d'InfoRoute Santé du Canada est de faire en sorte que d'ici 2010, la moitié des Canadiennes et des Canadiens aient un dossier de santé électronique à mettre à la disposition des fournisseurs de soins de santé.

Bien que les dossiers de santé électroniques présentent des avantages importants, comme l'accès rapide à des renseignements complets sur les patients pour les professionnels de la santé, ils comportent également un certain nombre de risques liés à la protection de la vie privée.

La protection de la vie privée doit être un facteur clé dans l'étude de la façon dont ces dossiers de nature hautement délicate sont gérés. Il est essentiel que les patients sachent ce qu'il advient des renseignements sur leur santé et qu'ils soient assurés de pouvoir exercer un contrôle sur ces renseignements.

Il faudra prévoir d'importantes mesures de sécurité pour protéger les dossiers de santé électroniques, y compris des mesures de protection pour veiller à ce que seules les personnes dûment autorisées puissent accéder aux renseignements qu'ils contiennent. Une attention particulière doit également être consacrée aux possibles usages secondaires des renseignements, y compris la recherche en santé.

La gestion des droits électroniques est l'expression courante pour désigner les diverses technologies utilisées pour faire respecter les règles préétablies d'utilisation du contenu numérique. Ces technologies englobent tout moyen par lequel des diffuseurs ou des fabricants contrôlent l'utilisation des données ou des équipements.

Si les technologies de gestion des droits électroniques se limitaient au contrôle de la copie et de l'utilisation du contenu, nous ne serions pas préoccupés outre mesure. Toutefois, ces technologies permettent de recueillir des renseignements personnels détaillés de la part des utilisateurs qui, bien souvent, accèdent au contenu par ordinateur. Ces renseignements sont communiqués au titulaire du droit d'auteur ou au fournisseur de contenu, à l'insu de l'utilisateur et sans son consentement.

Bien qu'existent des moyens de contourner ces technologies et, par conséquent, d'empêcher la collecte de renseignements personnels, les propositions de modification de la *Loi sur le droit d'auteur* antérieures comprenaient des mesures visant à interdire ce contournement.

Les technologies qui envoient à une entreprise des données sur l'utilisation d'un produit révèlent beaucoup d'information sur les goûts et les préférences des consommateurs. Ces données peuvent à vrai dire être extrêmement personnelles.

Le CPVP examinera attentivement les incidences sur la protection de la vie privée de toute mesure législative qui viserait à modifier la *Loi sur le droit d'auteur*.

Le dossier de santé électronique

Le gouvernement fédéral encourage la mise sur pied d'un système de dossiers de santé électroniques par l'intermédiaire du Partenariat fédéral pour les soins de santé.

Nous surveillons les progrès de ce groupe, dont les travaux pourraient avoir une incidence sur les services de soins de santé qui sont fournis aux Premières Nations et aux populations autochtones, aux anciens combattants admissibles, aux membres des Forces canadiennes, au personnel de la Gendarmerie royale du Canada (GRC), aux détenus sous responsabilité fédérale et aux demandeurs du statut de réfugié.

Le CPVP participe également activement au nouveau forum InfoRoute Santé du Canada – Protection de la vie privée, qui regroupe des représentants des ministères de la Santé et des bureaux de protection de la vie privée de tout le Canada. Le Forum permet de discuter de questions fondamentales de protection de la vie privée et de gouvernance qui doivent être étudiées de façon à assurer la réussite de la mise en œuvre du dossier de santé électronique.

Ces changements fourniront aux agents de police de nouveaux outils importants pour mettre un terme au vol d'identité ou à la fraude *avant* que les citoyens ne subissent un préjudice financier.

Un autre élément notable de la loi consiste en la possibilité que les délinquants soient contraints de dédommager les victimes. Cet élément est d'autant plus important qu'il s'agit d'une manière de reconnaître les graves répercussions financières qu'a le vol d'identité sur la personne.

Toutefois, nous sommes d'avis que ce projet de loi sur le vol d'identité n'est qu'un premier pas et que d'autres modifications législatives sont nécessaires.

Par exemple, l'une des principales questions que n'aborde pas le projet de loi C-27 est le faux-semblant, c'est-à-dire lorsqu'une personne obtient des renseignements personnels comme des données téléphoniques et financières en se faisant passer pour une personne autorisée à les détenir. Il faudra également légiférer en matière de pourriels, lesquels sont souvent utilisés par les voleurs d'identité pour tromper les personnes de manière à ce qu'elles fournissent leurs renseignements personnels en ligne. Le Canada est le seul pays du G-8 qui ne dispose pas de loi antipourriel.

AUTRES LOIS ET INITIATIVES AYANT UNE INCIDENCE SUR LA PROTECTION DE LA VIE PRIVÉE

Le droit d'auteur

Depuis quelques années, le gouvernement fédéral étudie des modifications à apporter à la *Loi sur le droit d'auteur*.

En janvier 2008, la commissaire à la protection de la vie privée a écrit aux ministres de l'Industrie et du Patrimoine canadien au sujet d'éventuelles modifications à la *Loi*.

Le CPVP est particulièrement préoccupé par le fait que certaines modifications autoriseraient l'utilisation de mécanismes techniques de prévention de la contrefaçon qui risquent d'avoir un effet négatif sur le droit à la vie privée des citoyens. Dans certains cas, les mécanismes de protection des produits visés par le droit d'auteur ont comme effet que des renseignements personnels sont recueillis, utilisés et communiqués sans le consentement des intéressés.

Des mesures techniques de protection peuvent être intégrées à divers médias afin de contrôler la copie et de prévenir la violation du droit d'auteur, ou elles peuvent être intégrées à des appareils électroniques afin d'empêcher la lecture de contenu non autorisé.

En février 2008, nous avons publié une résolution commune unanime qui énonce les mesures à prendre pour protéger la vie privée des Canadiennes et des Canadiens dont les renseignements personnels sont consultés dans le cadre d'un programme de PCA et la sécurité de ces renseignements.

Cette résolution insiste sur le fait que les citoyens canadiens disposent déjà d'un document d'identification de voyageur bien établi et hautement sécuritaire, en l'occurrence, le passeport canadien, mais reconnaît que certains pourraient vouloir une alternative.

Le vol d'identité

La nouvelle législation qui vise à résoudre le problème du vol d'identité représente un grand pas vers la résolution de ce crime de plus en plus courant.

Toutes les définitions de la vie privée renvoient à l'idée que les personnes doivent pouvoir exercer un contrôle sur ce qui est fait de leurs renseignements personnels et sur le moment et les fins auxquelles ils sont utilisés. Les victimes de vol d'identité ont manifestement perdu le contrôle de leurs renseignements personnels, ce qui entraîne des conséquences souvent graves et durables. Leur vie privée a été gravement atteinte.

Le vol d'identité est un problème complexe, causé par de nombreux facteurs.

Le projet de loi C-27 ciblait les premiers stades du vol d'identité et traitait des différentes manières qu'utilisent les criminels pour recueillir les renseignements personnels. Par exemple :

- Il rend illégal le fait d'avoir en sa possession ou de trafiquer des renseignements identificateurs si ces renseignements sont destinés à une utilisation frauduleuse.
- Il prévoit des dispositions contre une technique courante des voleurs d'identité, à savoir le détournement de courrier, en rendant illégal le fait de détourner de manière frauduleuse tout envoi par la poste et le fait de posséder une clé à courrier.
- Il prévoit des dispositions sur la fraude par carte de crédit par la création d'une nouvelle infraction de possession d'instruments de reproduction de renseignements de cartes de crédit.
- Il rend illégale l'obtention, la vente ou la possession de « documents d'identité » concernant une autre personne, offense pouvant entraîner une peine d'emprisonnement maximale de cinq ans.

gouvernement à également noté que la LPRPDE permet actuellement aux organisations de collaborer avec les organismes d'application de la loi et de sécurité nationale, sans nécessiter une assignation, un mandat ou une ordonnance d'un tribunal.

Avant de songer à instaurer des lois qui rendraient obligatoire la communication sur demande des renseignements personnels des clients, nous recommandons fortement que le gouvernement détermine si la clarification de la LPRPDE, ainsi que des lignes directrices appropriées, pourrait régler le problème.

L'accès légal soulève des questions fondamentales concernant les droits, comme le droit à la vie privée et le droit de communiquer librement. Le CPVP continuera de suivre cette question de près et de confier ses inquiétudes aux représentants du gouvernement et aux parlementaires.

Permis de conduire améliorés

En réponse aux plans d'étude ou de mise en œuvre des permis de conduire améliorés dans plusieurs provinces canadiennes, le CPVP et les gardiens de la vie privée dans les provinces et territoires expriment leur inquiétude en ce qui a trait aux risques pour la protection de la vie privée et la sécurité.

Ces permis de conduire améliorés sont la réponse des provinces à l'exigence qu'impose le gouvernement des États-Unis aux voyageurs de fournir une preuve de leur identité et de leur citoyenneté dans le cadre de l'Initiative relative aux voyages dans l'hémisphère occidental.

Ces développements ont soulevé des inquiétudes parmi les commissaires et les ombudsmans à la protection de la vie privée aux échelons fédéral, provincial et territorial. Une des principales préoccupations réside dans le fait que les renseignements personnels des conducteurs participants devraient demeurer au Canada et que des contrôles significatifs et indépendants de la façon dont la US Customs and Border Protection reçoit et utilise les renseignements personnels des Canadiennes et des Canadiens devraient être mis en place.

De plus, la technologie d'identification par radiofréquence (IRF) dans les permis de conduire améliorés (PCA) risque de porter atteinte à la vie privée, car elle pourrait permettre la localisation subreptice des personnes qui détiennent un PCA. Cette technologie pourrait aussi ne pas chiffrer ou protéger autrement le numéro d'identification unique de son détenteur et risquer de ne pas protéger les autres renseignements personnels qui pourraient être stockés dans le système d'IRF.

Le document de consultation ne permet pas de saisir la portée des difficultés qu'il cite. Est-ce 20 ou 80 pour cent des entreprises qui divulguent des renseignements volontairement? Les entreprises réagissent-elles en fonction du contexte, c'est-à-dire, en cas d'urgence lorsqu'il faut trouver le plus proche parent ou lorsqu'on soupçonne qu'il y a eu crime violent? Nous n'avons pas de réponse à ces questions cruciales.

Le Commissariat considère que le fait d'exiger de tous les fournisseurs de services de télécommunication qu'ils communiquent les renseignements personnels des clients sur demande est une solution trop large et peu adaptée pour un problème qui n'a pas clairement été défini ni mesuré.

Ni ce document de consultation ni les précédents n'ont présenté de justification convaincante, fondée sur des preuves empiriques, que l'incapacité d'obtenir les renseignements personnels des clients rapidement a causé des problèmes sérieux aux organismes responsables de l'application de la loi et de la sécurité nationale.

Même s'il était prouvé, documents et preuves empiriques à l'appui, que l'accès aux renseignements des clients pose problème, nous ne sommes toujours pas convaincus que le fait d'exiger des fournisseurs de services de télécommunication qu'ils communiquent ces renseignements sans mandat soit la seule, ni la meilleure, solution.

Nous sommes d'avis que les citoyens s'attendent raisonnablement au respect de leur vie privée lorsqu'ils fournissent des renseignements, ce qui met en doute la validité constitutionnelle de toute communication ou perquisition obligatoire.

Bien que le document de consultation mentionne l'absence de « dispositions législatives explicites » comme un problème à régler, la LPRPD offre en fait un code législatif explicite qui permet un accès légal aux organismes responsables de l'application de la loi et de la sécurité nationale tout en assurant la protection de la vie privée, ainsi que les autres droits et libertés des citoyens.

La LPRPD autorise les fournisseurs de services de télécommunication et d'autres organisations à communiquer aux organismes d'application de la loi des renseignements personnels sans le consentement des intéressés et sans mandat aux fins d'application de la loi ou de conduite d'une enquête. Elle permet également la communication sans consentement lorsqu'une situation d'urgence met en danger la vie, la santé ou la sécurité d'une personne.

L'accès légal a fait l'objet de nombreuses discussions pendant l'examen quinquennal de la LPRPD réalisé par le Comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique. Dans sa réponse, le gouvernement a mentionné la nécessité de clarifier le concept d'autorité légitime. Le

Les responsables de la protection des renseignements personnels du monde entier ont des préoccupations similaires quant à cette utilisation répandue des listes de personnes interdites de vol ainsi qu'à la collecte et à la communication de données sur les passagers. Les autorités de protection des données qui ont participé à la 29^e Conférence internationale des commissaires à la protection des données et de la vie privée, tenue à Montréal par le CPVP, ont appuyé une résolution exigeant des normes internationales pour l'utilisation et la communication des renseignements personnels des passagers recueillis par les transporteurs aériens.

La liste des personnes interdites de vol était aussi un point central de la présentation de la commissaire à la protection de la vie privée en novembre 2007 devant la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India. Nous avons prié la Commission d'enquête de tenir compte, lorsqu'elle évaluera la pertinence des mesures visant la sûreté du transport aérien, de la nécessité de doter le Canada de recours judiciaires, de mécanismes de protection exécutives et de systèmes de surveillance efficaces.

Accès légal

En octobre 2007, Sécurité publique Canada a publié un court document de consultation sur l'accès légal et les difficultés éprouvées par les organismes d'application de la loi à obtenir des renseignements sur les clients comme le nom, l'adresse, le numéro de téléphone ou l'adresse IP auprès des fournisseurs de services de télécommunication. Certaines entreprises communiquent volontairement cette information, alors que d'autres exigent qu'un mandat soit présenté avant de fournir l'information demandée, quelle que soit la nature de cette information ou le contexte entourant la demande. D'après le document de consultation de Sécurité publique Canada, cette situation complique le travail des agents de police, car ils ne disposent peut-être pas de moyens pour contraindre les organismes à divulguer les renseignements qu'ils recherchent.

Le document de consultation indique ce qui suit :

« Par exemple, les organismes d'application de la loi peuvent avoir besoin de l'information pour des raisons non reliées à une enquête (c.-à-d. pour trouver le plus proche parent en cas d'urgence) ou parce qu'il s'agit d'un début d'enquête. Le fait d'avoir accès à cette information de base constitue souvent la différence entre le début d'une enquête ou sa fin ».

semble-t-il, simplement parce que leur âge (10 et 15 ans) rendait évident le fait qu'ils ne constituaient pas une menace.

Un représentant de la compagnie aérienne a mis en garde une des familles en indiquant que leur fils aurait des problèmes chaque fois qu'il prendrait l'avion et lui a fait une suggestion radicale : changer de nom.

Le Programme de protection des passagers suppose l'utilisation secrète de renseignements personnels et, malgré cette grave atteinte au droit à la vie privée, les citoyens n'ont aucun droit exécutoire à un arbitrage indépendant, à une compensation financière pour les frais et autres dommages, ni à un quelconque recours en appel. Les citoyens n'ont même pas le droit de demander s'ils figurent sur la liste.

L'administration fédérale a fait savoir que la liste contient jusqu'à 2 000 noms. De toute évidence, il existe un risque important de faux positif – un problème qui s'est posé aux États-Unis, où des enfants et des personnalités publiques comme le sénateur Edward Kennedy ont été interrogés ou se sont vu refuser l'accès à bord.

Le Commissariat a clairement fait savoir qu'il ne s'opposerait pas à des initiatives qui protégeraient la vie des Canadiennes et des Canadiens. Toutefois, malgré nos demandes répétées, Transports Canada n'a toujours pas prouvé l'efficacité des listes de personnes interdites de vol.

Certains experts en sécurité ont suggéré que l'amélioration des inspections physiques dans les aéroports, y compris la vérification approfondie des bagages et du fret, serait une manière plus concrète et efficace d'améliorer la sûreté aérienne.

Une vérification des pratiques de gestion en matière de protection des renseignements personnels du Programme de protection des passagers est prévue.

NOTE : Vous trouverez de l'information sur notre examen de l'évaluation des facteurs relatifs à la vie privée du Programme de protection des passagers à la page 88.

Peu après l'entrée en vigueur de la liste des personnes interdites de vol, les commissaires à la protection de la vie privée et les ombudsmans des échelons fédéral, provincial et territorial ont demandé d'une seule voix au gouvernement fédéral de réviser en profondeur le

programme. Dans une résolution commune, nous avons demandé que le programme soit suspendu, ou du moins qu'il fasse l'objet d'une surveillance ministérielle étroite et que des rapports publics soient soumis régulièrement au Parlement jusqu'à ce qu'un examen parlementaire exhaustif soit réalisé.

Le droit à la vie privée est souvent malmené à mesure que de nouvelles mesures antiterroristes et d'application de la loi sont introduites. La tendance se poursuit des années après les attentats du 11 septembre.

Les citoyens s'attendent à ce que l'État prenne des mesures pour les protéger. Mais ils s'attendent aussi à ce que ces mesures respectent leurs droits, y compris le droit à la vie privée, et soient conformes à la primauté du droit, ce qui comprend les normes juridiques comme l'application régulière de la loi, le droit de consulter un avocat, le droit de connaître les preuves retenues ainsi que les autres éléments d'équité procédurale qui constituent la base de notre système de droit.

Voici un résumé des principales questions de sécurité nationale et d'application de la loi qui ont retenu l'attention en 2007-2008.

Liste des personnes interdites de vol

Après le 11 septembre 2001, l'attention s'est surtout portée sur la sûreté du transport aérien. Au Canada, la création d'une liste des personnes interdites de vol a soulevé de profondes inquiétudes non seulement en ce qui concerne le droit à la vie privée, mais aussi d'autres droits de la personne, comme la liberté d'association, la liberté d'expression et la liberté de circulation et d'établissement.

Les lacunes fondamentales du Programme de protection des passagers (la liste des personnes interdites de vol) ont été soulignées dès les premiers jours de son entrée en vigueur en juin 2007.

Deux jeunes Canadiens portant le même nom ont eu des démeles avec les autorités responsables des listes nord-américaines des personnes interdites de vol parce qu'ils avaient le même nom qu'une personne figurant sur une de ces listes.

Leur histoire est similaire : des alarmes se sont déclenchées lorsqu'ils se sont présentés aux guichets d'enregistrement des transporteurs aériens pour prendre leur avion. Les familles se sont fait dire qu'il y avait un problème de sécurité parce que le nom des garçons se trouvait sur une liste de personnes interdites de vol (sans qu'il soit précisé laquelle). Les deux jeunes n'ont pu prendre l'avion qu'après une longue attente, et ce,

Le droit à la vie privée est souvent malmené à mesure que de nouvelles mesures antiterroristes et d'application de la loi sont introduites. La tendance se poursuit des années après les attentats du 11 septembre.

Un élément essentiel du mandat du CPVP en vertu de la LPRP consiste à soutenir le travail du Parlement en l'informant et en le consultant sur les questions de protection de la vie privée.

Des initiatives concernant la sécurité nationale ont continué de soulever des préoccupations en ce qui a trait au droit à la vie privée en 2007-2008 et ont été au cœur de notre travail avec les députés et les représentants de nombreux ministères fédéraux. Parmi ces enjeux de sécurité nationale, mentionnons la liste canadienne des personnes interdites de vol, les consultations fédérales sur l'accès légal et les projets de permis de conduire améliorés dans certaines provinces.

Selon le Commissariat, un des points encourageants dans le domaine de l'application de la loi a été l'adoption de la mesure législative visant à contrer le vol d'identité. Le CPVP a également donné son avis sur de nombreux autres enjeux tout au long de l'année, y compris les modifications possibles à la *Loi sur le droit d'auteur* et la création de dossiers médicaux électroniques.

INITIATIVES D'APPLICATION DE LA LOI ET DE SÉCURITÉ NATIONALE

La régression que connaît le droit à la vie privée dans le monde depuis les attentats du 11 septembre 2001 n'est pas surfaite. Tous les États, y compris le Canada, ont répliqué par un large éventail d'initiatives de sécurité nationale, le plus souvent axées sur une collecte de plus en plus grande de renseignements sur les habitudes et les activités quotidiennes des gens ordinaires.

Les pouvoirs publics semblent croire que la sécurité nationale et publique repose sur la collecte, le tri et l'analyse de tonnes de données personnelles, sans jamais prouver

l'efficacité de telles mesures.



a plus de 40 accords d'échange de renseignements avec d'autres unités du renseignement financier sur des personnes soupçonnées de blanchiment d'argent ou de terrorisme. La LPRP ne reflète pas cette augmentation des échanges de renseignements à l'échelle internationale. Elle ne prévoit que deux restrictions à la communication de renseignements personnels aux États étrangers : un accord ou une entente doit exister et les renseignements personnels doivent être utilisés aux fins de l'administration ou de l'application d'une loi, ou de la tenue d'une enquête.

La Loi n'exige même pas que l'entente de partage de renseignements soit écrite, pas plus qu'elle n'impose d'exigences quant au contenu de ces ententes.

Les conséquences de la communication de renseignements personnels en l'absence de contrôles appropriés ont été clairement mises en relief par l'affaire *Maher Arar*.

Pendant la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, le juge O'Connor a conclu qu'il était très probable qu'en prenant la décision de détenir M. Arar et de le renvoyer en Syrie, les autorités américaines se sont fondées sur des renseignements inexacts sur M. Arar fournis par la GRC. Le juge O'Connor a émis une série de recommandations pour renforcer les politiques et pratiques de la GRC concernant le partage de renseignements avec d'autres instances gouvernementales.

Le gouvernement du Canada et le Parlement devraient envisager des dispositions particulières pour définir les responsabilités de ceux qui transmettent des renseignements personnels à d'autres administrations et pour aborder la question de l'efficacité de la protection des renseignements dans ces administrations.

Effet attendu

De bons contrôles sur la communication des renseignements permettraient d'atténuer les risques pour les citoyens. De meilleurs contrôles serviraient à veiller à ce que les renseignements partagés soient pertinents et exacts et à ce que les restrictions appropriées soient imposées, limitant l'utilisation des renseignements aux fins auxquelles ils ont été communiqués.

Conclusion

Ces 10 modifications simples permettraient d'entamer le processus d'harmonisation de la LPRP avec les lois modernes sur la protection des données ailleurs dans le monde. Le Commissariat espère que le Canada reprendra un jour le rôle de chef de file dans la promotion et la protection du droit à la vie privée qu'il avait lorsque la LPRP a été adoptée il y a près de 25 ans.

Effet attendu

Une couverture plus complète des enjeux relatifs à la gestion de la vie privée fournirait aux parlementaires l'information pertinente pour évaluer la mesure dans laquelle les institutions fédérales font face aux défis relatifs à la protection des renseignements personnels, et si les nouveaux programmes ou initiatives peuvent menacer le droit des citoyens à la vie privée. La population canadienne serait également mieux informée de la façon dont les ministères et organismes fédéraux traitent les renseignements personnels.

- 9 Incorporer une disposition exigeant des examens réguliers de la Loi sur la protection des renseignements personnels par le Parlement tous les cinq ans.

Contexte

Le paysage de la protection de la vie privée évolue continuellement. Il serait logique que le Parlement examine régulièrement la LPRP à la lumière des nouvelles technologies ou des nouvelles mesures fédérales qui pourraient avoir des répercussions sur le droit à la vie privée. Contrairement à la LPRP, la LPRPD prévoit un examen quinquennal de sa première partie. Quelques provinces prévoient également un tel examen de leur loi sur la protection des renseignements personnels applicable au secteur public.

Effet attendu

Un examen quinquennal obligatoire contribuerait à l'harmonisation du cadre canadien de protection des données dans l'ensemble des administrations du Canada. Il ferait en sorte que les décideurs canadiens et l'industrie canadienne gardent à l'esprit les pratiques en matière de protection des renseignements personnels des organismes des secteurs privé et public. Enfin, cet examen garantirait que la loi fédérale s'adapte aux tendances internationales ainsi qu'aux technologies en rapide évolution.

- 10 Renforcer les dispositions concernant la communication de renseignements personnels par le gouvernement canadien aux États étrangers.

Contexte

Grâce aux progrès technologiques, il est maintenant beaucoup plus facile et plus abordable pour les gouvernements de recueillir et de conserver des renseignements personnels sur les citoyens. Parallèlement, l'échange d'information entre les pays a augmenté de façon marquée, car les gouvernements ont adopté des approches plus concertées pour régir le déplacement des marchandises et des gens, ainsi que pour lutter contre la criminalité transnationale et le terrorisme international.

À titre d'exemple, l'Agence des services frontaliers du Canada partage de l'information douanière et des renseignements sur les voyageurs entrant au Canada avec d'autres pays, et le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE)

7 Amender la Loi sur la protection des renseignements personnels pour la faire concorder avec la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) en éliminant la restriction selon laquelle la Loi sur la protection des renseignements personnels ne s'applique qu'aux renseignements consignés.

Contexte

Les renseignements non consignés – comme ceux des caméras de surveillance qui n'enregistrent pas d'image – dépassent la portée de la LPRP. Les renseignements personnels que contient l'acide désoxyribonucleique (l'ADN) et d'autres échantillons biologiques ne sont pas explicitement visés par la Loi.

La LPRPDE, par contre, inclut toute forme de renseignements personnels.

Effet attendu

Élargir la définition de renseignements personnels permettrait de s'assurer que la LPRP prend en compte l'imagerie numérique et les applications biométriques liées aux activités contemporaines de surveillance et de contrôle de l'exécution de la loi, ainsi que de protéger l'ADN et les autres échantillons biologiques.

8 Renforcer les exigences touchant les rapports annuels des ministères et organismes gouvernementaux énoncées à l'article 72 de la Loi sur la protection des renseignements personnels en obligeant ces institutions à rendre compte au Parlement d'un plus large éventail de pratiques en matière de protection des renseignements personnels.

Contexte

La LPRP exige que chacun des responsables d'une institution fédérale soumette un rapport annuel au Parlement sur l'application de la Loi. Au fil des ans, notre expérience dans l'examen de ces rapports révèle que, dans l'ensemble, l'information qu'ils contiennent est rarement significative. Ces rapports sont davantage un collage de statistiques sur le nombre de demandes reçues dans le cadre de la LPRP, les dispositions prises à l'égard de ces demandes, les exemptions ou exclusions invoquées et les délais de traitement.

Le Secrétariat du Conseil du Trésor a publié en 2005 des lignes directrices détaillées à l'intention des institutions fédérales au sujet des rapports concernant la protection des renseignements personnels et il les a mises à jour en 2008. La LPRP devrait être modifiée de façon à intégrer aux exigences législatives ces lignes directrices afin de leur donner davantage de poids et d'autorité.

Les citoyens obtiendraient, en temps utile, l'information pertinente sur la façon dont les institutions fédérales traitent leurs renseignements personnels.

- 6 Conférer à la commissaire à la protection de la vie privée le pouvoir discrétionnaire de refuser ou d'abandonner une plainte dans les cas où une enquête ne serait guère utile et ne servirait aucunement l'intérêt public.

Contexte

Pour l'instant, l'obligation de faire enquête sur chacune des plaintes selon le principe du premier arrivé, premier servi accapare une quantité disproportionnée de précieuses ressources. Voici des exemples de types d'enquêtes qui donnent relativement peu de résultats concluants :

- Plaintes répétitives concernant des litiges qui ont déjà été tranchés dans des affaires antérieures (p. ex. concernant la collecte et l'utilisation légitimes des numéros d'assurance sociale).
- Plaintes devenues sans objet, dans le cas où une personne a, dans l'intervalle, reçu l'information demandée (p. ex. lorsque l'accès a déjà été accordé, quoiqu'avec un certain retard, strictement parlant, mais sans que cela ne désavantage la personne).

- Plaintes fréquentes déposées par une même personne contre une institution gouvernementale (p. ex. lorsque des litiges touchant le travail ou l'emploi constituent le motif réel du conflit).

- Plaintes multiples déposées par un grand nombre de plaignants concernant un même incident (p. ex. une importante atteinte à la sécurité de données).
- Problèmes qui ont déjà été recensés et réglés par une institution fédérale.

Plusieurs organismes chargés de la protection des données au Canada et ailleurs sont confrontés à des défis similaires. Ils doivent traiter indifféremment toutes les plaintes, sans pouvoir en rejeter ou en abandonner au début du processus, lorsque la tenue ou la poursuite d'une enquête ne servirait pas l'intérêt public.

Effet attendu

Cette latitude permettrait au Commissariat de concentrer davantage de ressources d'enquête sur les plaintes concernant la vie privée qui sont d'un intérêt systémique plus large et qui servent les intérêts d'un grand nombre de citoyens.

4 Modifier la Loi sur la protection des renseignements personnels pour confier au Commissariat un mandat clair en matière de sensibilisation du public.

Contexte

Bien que la fonction principale du CPVP selon la LPRP consiste à enquêter sur des plaintes et à les régler, il doit également faire progresser le droit à la protection de la vie privée par d'autres moyens, comme la recherche, les communications et la sensibilisation du public. Cependant, la Loi ne donne pas à la commissaire un mandat clair d'informer la population de ses droits en ce qui a trait à la protection des renseignements personnels que détiennent les institutions fédérales.

Effet attendu

Un mandat clair de sensibilisation du public donnerait au CPVP le pouvoir de publier des avis et des documents d'information sur les politiques et les mesures législatives importantes qui ont une incidence sur les renseignements personnels.

Comme la LPRPDE prévoit un tel mandat, il serait logique que la LPRP, qui s'applique au secteur public, fasse de même.

5 Donner au Commissariat une plus grande souplesse pour faire rapport publiquement sur les pratiques de gestion des renseignements personnels des institutions gouvernementales.

Contexte

Pour l'instant, le Commissariat informe le Parlement et la population par le biais de rapports annuels et de rapports spéciaux. Aucun article précis dans la législation n'autorise le CPVP à présenter des rapports pour des raisons d'intérêt public. Le Commissariat a été empêché de parler à la presse, au public et même aux députés en raison des contraintes qu'impose la LPRP en matière de confidentialité.

Devoir attendre la fin de l'exercice visé par le rapport pour communiquer aux citoyens les enjeux en matière de protection des renseignements personnels liés aux institutions fédérales dépourille l'information de sa portée pratique et la rend obsolète et peu pertinente. Un pouvoir clair de communication de l'information d'intérêt public permettrait des débats d'actualité pertinents sur les questions de protection de la vie privée qui sont importantes pour la population.

Effet attendu

Cette latitude serait un moyen efficace de sensibiliser le public, de lui fournir une assurance et, s'il y a lieu, de regagner sa confiance.

donc aucun recours efficace en cas d'atteinte à la vie privée, comme la communication ou la collecte induite de renseignements personnels.

Il s'agit d'une norme bien moins stricte que celle en vigueur dans le secteur privé, où la LPRPDE prévoit des recours pour les citoyens.

Effet attendu

L'élargissement du champ de compétence de la Cour fédérale permettrait de s'assurer que les institutions fédérales respectent le droit de chacun à ce que ses renseignements personnels soient recueillis, utilisés et communiqués de façon conforme à la LPRP. Ainsi, la LPRP serait comparable à la LPRPDE.

Pour avoir un sens, un droit doit s'accompagner d'un recours.

- 3 Inscrire dans la loi l'obligation, pour les responsables des institutions gouvernementales assujetties à la *Loi sur la protection des renseignements personnels*, d'effectuer une Évaluation des facteurs relatifs à la vie privée (ÉFVP) avant de mettre en œuvre un programme ou un système et d'en publier les résultats.

Contexte

En 2002, le Secrétaire du Conseil du Trésor a présenté une politique d'évaluation des facteurs relatifs à la vie privée (ÉFVP). Cette politique a été conçue pour garantir aux Canadiennes et aux Canadiens que l'on tiendrait compte des principes de protection des renseignements personnels dans l'élaboration et la mise en œuvre des programmes et services qui ont une incidence sur la vie privée.

Malheureusement, la mise en œuvre de la politique s'est faite de manière inégale. Comme notre rapport de 2006-2007 l'indique, une vérification par le CPVP a permis de constater que les ÉFVP ne sont pas toujours effectuées au moment opportun et qu'elles sont souvent réalisées bien après la mise en œuvre d'un programme, lorsqu'elles le sont.

Effet attendu

Imposer une obligation légale relative aux ÉFVP garantirait une réalisation systématique et opportune de ces études.

De plus, les ÉFVP devraient être soumises au Commissariat avant la mise en œuvre des programmes, ce qui permettrait au CPVP de formuler des recommandations aux institutions sur le meilleur moyen de protéger les renseignements personnels.

Voici une description des modifications rapides que propose le CPVP :

- 1 Instaurer par voie législative un « test de nécessité » pour les institutions gouvernementales qui recueillent des renseignements personnels, afin de les obliger à démontrer la nécessité de recueillir ces renseignements.

Contexte

Ce « test de nécessité » est déjà intégré aux politiques du Conseil du Trésor et à la LPRPDE. Il s'agit d'un principe de protection des renseignements personnels internationallement reconnu qui figure dans les législations modernes de nombreux pays. Par exemple, les provinces et les territoires ont adopté un modèle législatif visant le secteur public qui impose l'une des trois conditions suivantes : la collecte est expressément autorisée par un texte législatif, les renseignements sont recueillis aux fins de l'application de la loi, les renseignements sont directement liés à *et nécessaires* à un programme ou à une activité.

La LPRP actuelle stipule ce qui suit : « Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ». Ce libellé établit une norme qui n'est pas à la mesure des droits fondamentaux au cœur de la LPRP.

Effet attendu

L'intégration de meilleurs contrôles par l'institution qui recueille les renseignements permettra de réduire les risques de mauvaise utilisation et de communication des renseignements personnels.

- 2 Étendre les motifs de recours aux tribunaux en vertu de l'article 41 de la Loi sur la protection des renseignements personnels à toute la gamme des protections et droits relatifs à la vie privée que cette loi garantit et autoriser la Cour fédérale à allouer des dommages-intérêts à la charge des institutions contrevenantes.

Contexte

Actuellement, la Cour fédérale ne peut que réviser une décision de refus rendue par une institution fédérale à l'encontre d'une personne ayant demandé d'avoir accès à des renseignements personnels en vertu de la LPRP.

Bien que la commissaire puisse enquêter sur les plaintes qui concernent tout l'éventail des droits et protections garantis par la LPRP, ainsi que formuler des recommandations, si l'institution gouvernementale concernée ne donne pas suite aux recommandations de manière satisfaisante, ni la personne ni la commissaire ne peuvent demander à la Cour fédérale d'exiger l'application des recommandations ou d'accorder un recours. Il n'existe

Puisque le gouvernement semble peu enclin à remanier la législation, la commissaire a présenté au Comité, en avril 2008, 10 modifications rapides à apporter à la Loi. Ces changements relativement simples complétaient certaines lacunes, notamment en instaurant un « test de nécessité » pour la collecte de renseignements personnels par les ministères.

Cependant, ces propositions ne tiennent absolument *pas* lieu de déclaration définitive sur la réforme de la LPRP. Le Commissariat considère ces 10 recommandations comme une première étape vers un remaniement en profondeur.

Le Commissariat considère ces 10 recommandations comme une première étape vers un remaniement en profondeur.

Certains des changements proposés ne feraient qu'incorporer à la loi des politiques et des pratiques fédérales déjà existantes. Le Secrétaire du Conseil du Trésor a fait du bon travail sur les questions de protection des renseignements personnels en fournissant des directives aux ministères responsables, sur la signature d'accords de partage de renseignements et sur l'impartition du traitement des renseignements personnels, par exemple. Toutefois, une modification de la loi assurerait l'existence d'orientations plus claires en cette matière.

D'autres changements proposés correspondent à des dispositions déjà présentes dans la LPRPPE ou qui sont à l'étude.

Dix modifications rapides à apporter à la LPRP

- 1 Instaurer un « test de nécessité » obligeant les institutions gouvernementales à prouver qu'elles ont besoin des renseignements personnels qu'elles recueillent.
- 2 Étendre les motifs de recours aux tribunaux en vertu de l'article 41 de la Loi sur la protection des renseignements personnels et autoriser la Cour fédérale à allouer des dommages-intérêts à la charge des institutions contrevenantes.
- 3 Rendre obligatoire l'évaluation des facteurs relatifs à la vie privée (EFVP) d'un programme avant sa mise en œuvre ainsi que la publication des résultats.
- 4 Prévoir un mandat clair de sensibilisation du public.
- 5 Assurer une plus grande latitude dans la publication de rapports sur les pratiques de gestion des renseignements personnels des institutions gouvernementales.
- 6 Accorder le pouvoir discrétionnaire de refuser ou d'abandonner une plainte lorsqu'une enquête ne sert pas l'intérêt public.
- 7 Éliminer la restriction selon laquelle la LPRP ne s'applique qu'aux renseignements considérés.
- 8 Obliger les institutions gouvernementales à rendre compte annuellement d'un plus large éventail de pratiques de protection des renseignements personnels.
- 9 Exiger une révision quinquennale de la LPRP par le Parlement.
- 10 Renforcer les dispositions qui régissent la communication par l'administration fédérale de renseignements personnels aux États étrangers.

LE POINT SUR LA RÉFORME DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : PREMIERS PAS VERS UNE REFORME

Le CPVP propose une série de modifications pour améliorer rapidement la loi sur la protection des renseignements personnels applicable au secteur public. Les commissaires à la protection de la vie privée demandent depuis de nombreuses années une réforme de la *Loi sur la protection des renseignements personnels* (LPPRP), et la nécessité toujours plus pressante de moderniser la législation est devenue un thème récurrent dans nos rapports annuels.

Cette année ne fait pas exception. La législation actuelle ne protège pas adéquatement les renseignements personnels des Canadiennes et des Canadiens qui sont en la possession des ministères et organismes fédéraux.

En 2006, le Commissariat a publié un rapport détaillé sur les changements qui devraient être apportés à la LPPRP.

Depuis, nous avons consulté des intervenants externes sur la question. Nous avons notamment demandé au Forum des politiques publiques d'organiser deux tables rondes sur la réforme du régime fédéral de protection des renseignements personnels, en juin et en octobre 2007, auxquelles ont participé de hauts fonctionnaires fédéraux qui prennent part à la promotion et à la protection du droit à la vie privée.

Pendant la préparation du présent rapport, nous avons eu vent de l'intention du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes de se pencher sur la LPPRP.

Le Comité a entendu de nombreux témoins. Le Commissariat espère que les membres du Comité reprendront ces travaux à l'automne 2008.

les institutions fédérales soient gérées sans problème majeur ni complications inattendues. Les pratiques exemplaires des institutions fédérales, ainsi que celles des provinces, des administrations étrangères et du secteur privé, devraient faire partie intégrante du programme de formation.

Conclusion

L'administration fédérale ne doit pas hésiter à répondre aux besoins de ses employés en ce qui a trait à la formation et à l'apprentissage sur la protection des renseignements personnels. Elle doit le faire immédiatement avant qu'un incident regrettable ne se produise, comme au Royaume-Uni.

Les fonctionnaires qui gèrent les renseignements personnels des Canadiennes et des Canadiens sont les gardiens de la confiance du public, base de notre régime politique.

Ils doivent avoir une profonde connaissance des lois, règles, règlements et politiques qui régissent la protection de la vie privée et la gestion des renseignements personnels au sein de l'administration fédérale. Ils doivent avoir une bonne compréhension de ce en quoi consistent les renseignements personnels, des principes de base de la protection de la vie privée et des pratiques équitables dans le domaine des renseignements personnels, ainsi qu'une bonne connaissance des meilleures pratiques de gestion des renseignements personnels.

Ces connaissances spécialisées ne peuvent s'acquérir que grâce à un programme de formation complet et concerté pour tous les fonctionnaires fédéraux qui gèrent des renseignements personnels. Le Secrétaire du Conseil du Trésor et l'École de la fonction publique du Canada ont un rôle de chef de file à jouer dans l'acquisition de ces connaissances. Les sections de l'AIPRP des ministères et organismes doivent également jouer un grand rôle, car elles sont les plus appropriées pour transmettre le savoir nécessaire au personnel de chacun des ministères et organismes.

Le CPVP demeure prêt à apporter son aide à tous ces joueurs dans l'élaboration d'un programme de formation sur la protection des renseignements personnels destiné à l'administration fédérale.

Une perspective globale sur la formation et l'apprentissage en matière de protection des renseignements personnels est un des éléments clés de la protection des renseignements personnels des Canadiennes et des Canadiens.

Contenu de la formation

Conformément à la recommandation du CPVP dans le cadre de la vérification de l'Agence des services frontaliers du Canada, chaque institution fédérale devrait envisager de mettre sur pied un comité de gestionnaires chargé de veiller à ce que l'orientation et la formation nécessaires en matière de protection des renseignements personnels soient fournies aux secteurs des programmes.

Le principal objectif d'un programme de formation sur la protection des renseignements personnels devrait être de donner aux fonctionnaires les bases des exigences fédérales en matière de protection des renseignements personnels que conserve l'État, et de leur faire connaître les pratiques exemplaires dans le domaine de la gestion des renseignements personnels.

Afin d'y arriver, un programme de formation en protection des renseignements personnels à l'intention des fonctionnaires devrait porter sur les thèmes et les sujets clés suivants :

- **Exigences des lois et des politiques** : Les fonctionnaires doivent connaître leurs devoirs et leurs responsabilités dans le cadre de la LPRP et des dispositions des règlements et autres textes réglementaires qui concernent la protection des renseignements personnels. (Les ministères et organismes devraient devoir adapter leurs programmes de formation en fonction des exigences qui les concernent selon la loi qu'ils administrent et de leurs politiques internes de gestion de données.)
- **Définition de renseignements personnels** : Les fonctionnaires qui gèrent des renseignements personnels doivent disposer de solides bases sur la définition des renseignements personnels (renseignements, quels que soient leur forme et leur support, concernant un individu identifiable) et ce qu'ils comprennent.
- **Principes de base** : Les fonctionnaires fédéraux doivent savoir quels renseignements personnels ils peuvent recueillir, utiliser et communiquer dans le cadre de leurs fonctions. Ils doivent aussi savoir comment conserver ces renseignements personnels de manière sécuritaire. La connaissance des principes de base de la protection des renseignements personnels – souvent appelés « principes relatifs à l'équité dans le traitement des renseignements personnels » – est essentielle.
- **Pratiques exemplaires** : Certains processus, techniques et méthodes sont mieux que d'autres quand il s'agit d'atteindre des résultats positifs en matière de promotion et de protection des renseignements personnels. Permettre aux fonctionnaires de développer une solide connaissance de ces techniques permettra de veiller à ce que les renseignements personnels des Canadiens et des Canadiennes que conservent

L'élaboration d'un programme de base, d'un module de formation et d'un guide des formateurs devrait être menée en collaboration avec le Commissariat à la protection de la vie privée et le Commissariat à l'information.

Le rôle des sections de l'AIPRP

Nous croyons que chaque section de l'AIPRP devrait jouer un rôle de premier plan dans la formation des employés et des superviseurs au sein de son ministère ou organisme.

Le programme de base et le guide des formateurs préparés par l'EBPC et décrits ci-haut seraient à la base de la formation. Nous reconnaissons, toutefois, que les besoins en matière de formation peuvent varier d'un ministère ou organisme à l'autre. En effet, les institutions qui traitent de grandes quantités de données personnelles, comme l'Agence du revenu du Canada ou l'Agence des services frontaliers du Canada, auront des besoins différents de ceux d'un ministère qui, en comparaison, traite peu de renseignements personnels, comme le ministère des Finances. Nous croyons donc que les ministères et organismes devraient pouvoir adapter le programme de base et le guide des formateurs à leurs propres besoins et contextes.

Le rôle du Secrétariat du Conseil du Trésor

Le SCT est chargé de l'administration de la LPRP à l'échelle du gouvernement. Il en coordonne l'administration en rédigeant et en distribuant des politiques et des lignes directrices visant à aider les institutions à interpréter la Loi et à la mettre en application à l'égard de questions de premier plan.

Nous croyons que le SCT devrait rendre obligatoire la formation décrite ci-haut pour l'ensemble de la fonction publique fédérale. En effet, le SCT doit être un chef de file en ce qui a trait à la promotion et à la supervision de la formation et de la sensibilisation en matière de protection des renseignements personnels pour l'ensemble de la fonction publique fédérale. Il ne faut pas sous-estimer son rôle et son importance en ce qui concerne la mise en place d'une culture de protection de la vie privée au sein de la fonction publique.

Nomination de « champions de la formation sur la protection des renseignements personnels »

Chaque ministère et organisme devrait envisager de nommer un « champion de la formation sur la protection des renseignements personnels » chargé de superviser et de promouvoir la formation et l'apprentissage en la matière dans son institution. Cette personne devrait être un membre de la haute direction, par exemple le responsable de la protection de la vie privée de l'organisme.

Le ministère des Affaires étrangères et du Commerce international a mis sur pied une politique, un processus et un programme de formation permanents pour veiller à ce que tous les analystes de l'information et de la protection des renseignements personnels reçoivent la formation nécessaire à l'exercice de leurs fonctions. Cependant, le Ministère est convaincu de la nécessité pressante d'offrir de la formation à plus grande échelle.

De toute évidence, certains ministères souhaitent répondre à la demande à l'aide de programmes proactifs qui officialiseraient la formation sur la protection des renseignements personnels. Mais pour combler les besoins en formation, il leur faut davantage de soutien.

Une approche globale

Le Commissariat est d'avis qu'une stratégie concertée et globale doit être élaborée et mise en œuvre par les intervenants fédéraux clés : l'École de la fonction publique du Canada (EFPC), le Secrétariat du Conseil du Trésor (SCT), et les bureaux de l'AIPRP dans chacun des ministères et organismes fédéraux.

Le rôle de l'École de la fonction publique du Canada

Le principal mandat de l'EFPC consiste à s'assurer que tous les employés de la fonction publique ont les connaissances et les compétences nécessaires pour élaborer des politiques et fournir des services aux Canadiennes et aux Canadiens.

Nous croyons que l'EFPC devrait élaborer un programme obligatoire de formation de base sur la protection des renseignements personnels que tous les ministères et organismes gouvernementaux pourraient utiliser pour la formation des employés qui traitent de grandes quantités de renseignements personnels. Le public cible de ce programme de base irait des employés aux superviseurs. Des modules d'enseignement et un guide des formateurs devraient être élaborés en collaboration avec les principales institutions gouvernementales à Ottawa qui traitent de grandes quantités de renseignements personnels.

L'EFPC devrait également élaborer un module distinct de formation obligatoire pour tous les cadres intermédiaires et supérieurs en vue de leur transmettre les bases de la gestion et de la protection des renseignements personnels. Ce module pourrait être intégré aux cours actuels destinés aux cadres ou offert seul, au besoin. (Si l'EFPC offre présentement deux modules de formation sur les lois qui concernent la protection des renseignements personnels et l'accès, ils ne sont pas obligatoires et visent les spécialistes fonctionnels et les superviseurs, ainsi que les gestionnaires.)

Une vérification des activités de Passeport Canada, évoquée précédemment, a également mis en relief à quel point l'absence de formation adéquate peut conduire à des risques pour la protection des renseignements personnels et pour la sécurité.

Un programme de base

Certains ministères et organismes fédéraux ont reconnu l'importance d'offrir au personnel une meilleure formation sur la protection des renseignements personnels. Statistique Canada ainsi que Citoyenneté et Immigration Canada ont mis sur pied des programmes de formation et donné des directives officielles pour attirer l'attention sur les enjeux et la législation liés à la vie privée. Depuis quelques années, le Secrétaire du Conseil du Trésor offre lui aussi de la formation à la communauté de l'AIPRP. De plus, le Secréariat donne en permanence des conseils sur des enjeux spécifiques liés à la protection de la vie privée aux responsables de l'AIPRP et aux responsables de programmes des institutions.

Malgré ces réussites, nous croyons que, dans l'ensemble, l'administration fédérale pourrait en faire bien davantage.

Une partie du problème relève du fait qu'il n'existe aucun programme de base obligatoire pour sensibiliser les fonctionnaires chargés du traitement ou de la gestion des renseignements personnels quant à leurs devoirs et responsabilités de base qui découlent de la LPRP. Et il n'existe pas non plus de programme obligatoire de formation de base de ces employés sur les principes largement reconnus d'équité dans le traitement des renseignements personnels qui régissent la collecte, l'utilisation, la communication et le retrait appropriés des renseignements personnels conservés par l'État.

L'École de la fonction publique du Canada offre deux modules de formation sur la *Loi sur la protection des renseignements personnels* et la *Loi sur l'accès à l'information*, mais ils ne sont pas obligatoires. (Les deux cours actuels seront regroupés en un nouveau cours débutant au début de 2009.)

Beaucoup de ministères et d'organismes ont élaboré leurs propres programmes de formation, mais dans la plupart des cas ces formations sont insuffisantes.

La Commission de la fonction publique du Canada (CFP), par exemple, tient des séances d'information pour conseiller et former ses cadres quant à l'incidence de la LPRP sur les divers programmes. Les séances sont si populaires que la CFP a dû refuser certains de ses cadres en 2007 en raison du manque de ressources pour donner la formation. Depuis, la CFP a étendu le programme pour essayer de répondre à la demande.

En octobre 2007, le Commissariat a publié les conclusions d'une vérification sur l'efficacité et les résultats des évaluations des facteurs relatifs à la vie privée (EFVP) des programmes et services, nouveaux ou redéfinis, effectuées par les ministères et les organismes fédéraux.

Une des principales conclusions de cette vérification aborde la nécessité d'offrir davantage de formation pour veiller à ce que les gestionnaires de programme comprennent leurs responsabilités au regard de la Politique d'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor et qu'ils aient les connaissances et la compétence nécessaires pour faire des EFVP efficaces.

Alors que certaines institutions gouvernementales ont déployé de sérieux efforts pour appliquer la politique, davantage de mesures s'imposent pour que les EFVP aient l'effet désiré, dont faire de la protection de la vie privée une considération fondamentale dans la prestation des programmes et des services fédéraux. La vérification a également permis de constater une application inégale de la politique et de nombreuses lacunes sur le plan du rendement. Les vérificateurs attribuent ces résultats décevants à de nombreux facteurs, dont le manque de formation.

Une autre vérification importante, décrite en détails dans notre rapport annuel 2005-2006, a permis d'examiner les pratiques de gestion de l'Agence des services frontaliers du Canada (ASFC) en ce qui a trait à la circulation transfrontalière des données et a révélé des problèmes similaires concernant les besoins en formation du personnel clé.

De façon générale, la vérification a permis de déterminer que l'ASFC dispose de plusieurs options pour assurer une meilleure gestion des risques associés à la protection de la vie privée et mieux veiller à son obligation de rendre des comptes, à être plus transparente et à mieux contrôler la circulation transfrontalière des renseignements personnels. La vérification a fait ressortir la nécessité d'offrir régulièrement des séances de formation sur l'application et le respect de la LPRP. Elle recommande à l'ASFC d'élaborer et de mettre en œuvre un cadre de gestion de la protection de la vie privée, dont un élément serait l'établissement d'un comité de cadres supérieurs chargé de veiller à ce que l'orientation et la formation en matière de protection des renseignements personnels soient fournies.

Enfin, la vérification recommande l'élaboration de modules de formation qui traiteraient particulièrement des problèmes liés à l'échange verbal de renseignements personnels entre les autorités frontalières du Canada et des États-Unis.

Cette formation sur la protection de la vie privée devrait être obligatoire pour tous les cadres et tous les fonctionnaires qui traitent des renseignements personnels.

La commission a également souligné l'absence totale de systèmes significatifs, une très mauvaise compréhension de l'importance que revêt le traitement des données et une philosophie du « on se débrouille comme on peut ». Selon la commission, le personnel travaillait au jour le jour sans le soutien, la formation ou les directives nécessaires pour traiter convenablement les renseignements personnels de nature délicate.

À la suite de l'atténuation de la protection des données, le gouvernement britannique a mis en place une formation annuelle obligatoire pour tous les fonctionnaires qui traitent des données personnelles.

Au Canada, le CPVP presse depuis un certain temps l'administration fédérale de fournir aux fonctionnaires une meilleure formation sur les principes de base de la gestion des renseignements personnels. Cette formation sur la protection de la vie privée devrait être obligatoire pour tous les cadres et tous les fonctionnaires qui traitent des renseignements personnels.

Si les programmes de formation adéquats ne sont pas mis en place, un incident regrettable pourrait mener à une atténuation de la protection des renseignements personnels détenus par un ministère ou un organisme fédéral. Un tel incident risque d'avoir des conséquences pour des milliers, voire des millions, de Canadiennes et de Canadiens.

Depuis quelques années, de nombreuses atténuations importantes à la protection des renseignements personnels ont eu lieu partout dans le monde, dans les secteurs privé et public.

Ces atténuations prennent souvent l'allure d'une perte de renseignements personnels résultant de l'inattention ou de la négligence d'un employé, ou encore d'un vol de matériel contenant des données. Dans un grand nombre de ces situations, les atténuations à la protection des renseignements personnels auraient pu être évitées si les personnes qui traitaient les données avaient eu une formation sur les principes de base d'une gestion sécuritaire et responsable des renseignements personnels.

Préoccupations relatives aux vérifications

De récentes vérifications du CPVP ont fait ressortir la nécessité d'une formation complète sur la protection des renseignements personnels pour les employés qui traitent ces renseignements dans les ministères et les organismes fédéraux.

FORMATION SUR LA PROTECTION DE LA VIE PRIVÉE DANS LA FONCTION PUBLIQUE FÉDÉRALE : NÉCESSITÉ D'UNE PERSPECTIVE GLOBALE

Un des moyens clés de prévenir les atteintes à la protection des données est de donner une formation sur la protection des renseignements personnels aux employés qui les traitent.

Vers la fin de 2007, une erreur relativement banale d'un fonctionnaire britannique a mené à l'une des plus grosses atteintes à la protection des données de l'histoire. L'incident a compromis les renseignements personnels de 25 millions de bénéficiaires de prestations pour enfants. Il s'agit d'un avertissement pour les gouvernements du monde entier quant à la nécessité de considérer avec le plus grand sérieux la protection des données, y compris la formation des employés en la matière.

Un fonctionnaire de l'Agence responsable du revenu et des douanes au Royaume-Uni a mis deux disques qui renfermaient des renseignements sur des familles inscrites à un fichier de prestations pour enfants dans une enveloppe destinée à un autre ministère.

Les CD ne sont jamais parvenus à destination et n'ont toujours pas été retrouvés.

Cette atteinte à la protection des données, qui a exposé des familles de partout au Royaume-Uni au risque de se faire voler leur identité, a conduit à la démission du président de l'Agence responsable du revenu et des douanes et à une importante enquête policière.

Après l'enquête, la British Independent Police Complaints Commission a conclu que les membres du personnel n'étaient pas responsables à titre individuel. Elle a plutôt indiqué que ce sont des pratiques et des procédures de traitement de données « absolument inadéquates » et l'absence de formation du personnel qui sont à l'origine de cette atteinte à la protection des renseignements personnels.



politique solide et efficace qui protégera mieux la vie privée des Canadiennes et des Canadiens.

La tendance de l'administration fédérale à mettre en ligne de plus en plus d'information soulève des questions cruciales sur l'équilibre entre l'intérêt public et le droit à la vie privée de chacun.

Certes, l'utilisation d'Internet est une évolution positive qui favorise la transparence et l'obligation de rendre des comptes au sein de l'administration fédérale (publication des contrats ou des frais de déplacement), mais lorsqu'il s'agit de communiquer des renseignements personnels, il faut indéniablement des limites.

Prochaines étapes

Les dispositions de la LPRP ne nous permettent pas de soumettre la question aux tribunaux pour obtenir conseil.

Toutefois, le Commissariat entend poursuivre son travail avec les institutions gouvernementales qui se sont montrées réticentes à mettre en œuvre toutes les recommandations. Nous espérons qu'un dialogue constructif permettra de convaincre ces institutions de prendre les mesures nécessaires pour protéger la vie privée des Canadiennes et des Canadiens.

Nous espérons qu'un dialogue constructif permettra de convaincre ces institutions de prendre les mesures nécessaires pour protéger la vie privée des Canadiennes et des Canadiens.

Nous croyons également qu'une nouvelle politique nationale sur cette question est nécessaire. Étant donné la complexité des enjeux, les recommandations qui découlent des enquêtes sur un petit nombre d'institutions ne sont pas les meilleures bases pour créer des mécanismes visant à assurer le respect de la LPRP à l'échelle de l'administration fédérale. L'élaboration d'une politique globale fondée sur des consultations auprès d'un plus grand nombre d'institutions fédérales est nécessaire.

Nous avons déjà indiqué au Secrétaire du Conseil du Trésor que nous croyons qu'une politique commune est nécessaire. Une politique commune garantirait l'uniformité dans la protection des renseignements personnels des Canadiennes et des Canadiens qui participent aux procédures administratives et quasi judiciaires.

Beaucoup d'institutions sur lesquelles le CPVP a enquêté partagent notre avis qu'une politique commune est nécessaire et l'accueilleraient favorablement. Elles sont disposées à participer à des consultations avec le Conseil du Trésor pour définir les orientations d'une politique, puis à s'y conformer une fois la politique en vigueur.

Le Conseil du Trésor a fait savoir au Commissariat qu'il travaille toujours à l'élaboration d'orientations pour les institutions fédérales qui publient un contenu assujéti à la LPRP sur les sites Web fédéraux. De plus, il a indiqué qu'il nous consulterait pour les versions préliminaires de toute politique qu'il serait susceptible d'élaborer.

La publication électronique de renseignements personnels dans les décisions administratives et quasi judiciaires des institutions gouvernementales est une affaire risquée en matière de protection de la vie privée. Nous sommes enthousiastes à l'idée de travailler avec le Conseil du Trésor sur cet enjeu important qu'est la mise en place d'une

décisions d'Internet ou encore les dépersonnaliser suffisamment en utilisant des initiales au hasard, dans un délai raisonnable.

Réponse aux préoccupations du CPVP

Même après avoir été avisées de problèmes relatifs à la protection de la vie privée, la plupart des institutions fédérales étaient réticentes à changer leurs politiques et leurs pratiques.

En dépit de la quantité et de la gravité croissantes des menaces pour la vie privée des personnes dont les renseignements personnels sont publiés sans discernement sur Internet, quelques institutions fédérales nous ont indiqué qu'elles prévoient continuer de publier des renseignements personnels de nature délicate comme elles l'ont toujours fait. D'autres institutions ont pris des mesures importantes, quoiqu'insuffisantes, pour améliorer la conformité à la LPRI. À la suite de nos enquêtes, des institutions ont mis en œuvre des mesures techniques pour empêcher que les principaux moteurs de recherche ne génèrent, lorsqu'une requête est effectuée, des documents qui contiennent le nom des personnes qui participent au processus décisionnel. D'autres ont convenu d'utiliser des initiales au lieu du nom complet.

Service Canada et Développement des ressources humaines Canada, quant à eux, ont consenti à mettre en œuvre toutes nos recommandations. Le CPVP a transmis les résultats de ses enquêtes aux plaignants. Dans les cas où les résultats étaient décevants, le Commissariat demeure déterminé à travailler avec les organismes en question afin d'améliorer la protection de la vie privée des personnes qui participent aux processus administratifs et quasi judiciaires. Les différents degrés de réceptivité aux recommandations du CPVP signifient que même les tribunaux qui ont fait l'objet d'une enquête ne protègent pas de façon uniforme les renseignements personnels des Canadiennes et des Canadiens qui participent à des actions en justice.

Par ailleurs, il est intéressant de noter que beaucoup d'autres organismes administratifs et quasi judiciaires publient en ligne des motifs de décisions qui permettent de relier des personnes identifiables à une grande quantité de renseignements personnels de nature délicate, mais que personne ne s'en est plaint auprès du CPVP.

judiciaire, les renseignements personnels présentés devant un tribunal deviennent, aux termes de la LPRP, d'ordre public.

Cependant, aucune de ces institutions n'a pu soumettre une quelconque preuve que les renseignements personnels communiqués pendant une procédure judiciaire sont accessibles au grand public. Le Commissariat a conclu que la communication de renseignements personnels pendant une audience ne suffisait pas à rendre ces renseignements d'ordre public.

La LPRP permet aussi la communication de renseignements personnels dans le cadre d'une loi fédérale ou d'un règlement qui l'autorise.

Certaines institutions ont soutenu que la communication de renseignements personnels était permise puisque la législation pertinente ne l'interdit pas ou ne prévoit aucune mesure. Nous avons rejeté cet argument. Une loi ou un règlement doit préciser si l'intention du Parlement était de permettre la communication de renseignements personnels en dehors du régime quasi constitutionnel que crée la LPRP. Le silence de la loi sur la question ne constitue pas une autorisation légale de communiquer des renseignements personnels.

Recommandations

En ce qui concerne les enquêtes sur les plaintes fondées, le Commissariat a fait quelques recommandations aux institutions gouvernementales :

- Dépersonnaliser suffisamment les décisions futures qui seront publiées sur Internet en utilisant des initiales au hasard au lieu du nom des personnes ou en ne publiant qu'un résumé de la décision qui serait exempt de renseignements personnels permettant d'identifier les personnes.

- Respecter les lignes directrices suggérées concernant l'exercice du pouvoir discrétionnaire quant à la communication de renseignements personnels dans les affaires où une institution a l'intention de communiquer des renseignements personnels dans les versions électroniques des décisions publiées sur Internet.

- Retirer d'Internet en priorité les décisions qui sont à l'origine des plaintes déposées devant le CPVP jusqu'à ce qu'elles soient suffisamment dépersonnalisées par l'utilisation d'initiales au hasard pour être remises ensuite en ligne conformément à la LPRP.

- Limiter dans les moteurs de recherche mondiaux l'indexation par nom des décisions antérieures grâce à un « fichier d'exclusion des robots » approprié ou retirer les

Limites de la loi sur la protection des renseignements personnels

Au cours des enquêtes, nous avons découvert une absence significative de consensus entre les décideurs administratifs et quasi judiciaires relativement aux limites que la LPRP prévoit quant à la communication de renseignements personnels dans les décisions publiées sur Internet.

Les décisions de la plupart, voire de la totalité, des institutions assujetties à la LPRP contiennent le type de renseignements personnels protégés par la loi.

La LPRP stipule que les renseignements personnels qui relèvent d'une institution fédérale peuvent être communiqués aux fins pour lesquelles ils ont été recueillis ou préparés, ou pour les usages qui sont compatibles avec ces fins.

Le CPVP a conclu que la communication électronique complète des motifs de décisions de ces organismes dans un intranet ou sur Internet ne correspond pas aux fins pour lesquelles les renseignements ont été obtenus. Les tribunaux recueillent plutôt des renseignements personnels pour rendre des décisions en se fondant sur les faits établis dans chaque affaire particulière dont ils sont saisis.

De plus, la communication systématique sur Internet des décisions administratives ou quasi judiciaires contenant des renseignements personnels permettant d'identifier les personnes n'a pas été jugée raisonnablement nécessaire pour la réalisation des mandats des institutions ayant fait l'objet d'une enquête. Il ne s'agissait pas d'une communication destinée à un usage conforme aux fins pour lesquelles les renseignements avaient été obtenus, notamment lorsque l'usage qui serait fait des renseignements personnels de nature délicate ne pouvait pas être déterminé à l'avance ni contrôlé.

En vertu de la LPRP, les limites à la communication de renseignements personnels ne concernent pas les renseignements auxquels le public a accès. Certaines des institutions sur lesquelles nous avons enquêté ont avancé qu'étant donné la nature publique d'une procédure administrative ou quasi

La communication
systématique sur
Internet des décisions
administratives ou quasi
judiciaires contenant
des renseignements
personnels permettant
d'identifier les personnes
n'a pas été jugée
raisonnablement
nécessaire pour la
réalisation des mandats
des institutions ayant fait
l'objet d'une enquête.

L'avancement des valeurs qui sous-tendent le principe de l'audience publique ne sera pas entravé si, conformément aux obligations que la LPRP impose aux institutions gouvernementales, ne sont publiées que les décisions dépersonnalisées, qui ne révèlent pas l'identité des participants. En outre, les tribunaux peuvent également décider de retrancher tous les renseignements personnels qui pourraient autrement apparaître dans les motifs des décisions, auxquels peut accéder le public. Toutefois, supprimer tout simplement les identifiants directs et évidents, comme les noms, est probablement le moyen le plus efficace et efficient de se conformer à la LPRP. Cette méthode de protection de la vie privée ne présente pas de risque important pour l'indépendance des tribunaux et permet d'assurer que les faits et les questions liés à des cas personnels peuvent être débattus de manière exhaustive et transparente dans un climat d'ouverture et d'accessibilité.

Lorsqu'un intérêt d'ordre public réel et impératif de communiquer des renseignements permettrait d'établir l'identité l'emporte nettement sur l'invasion de la vie privée, les institutions disposent de l'autorité nécessaire pour juger de la pertinence de communiquer des renseignements personnels de façon explicite dans leurs décisions. Par exemple, quand le public veut connaître l'identité d'une personne reconnue coupable devant une instance disciplinaire, ou qui est susceptible de représenter un danger pour le public, le tribunal peut exercer son pouvoir discrétionnaire pour communiquer des renseignements personnels au public, y compris le nom de la personne en question.

Dans le même ordre d'idées, si le Parlement ou tout autre organisme habilité à adopter des règlements a établi une loi ou un règlement qui autorise la communication de renseignements personnels, la LPRP permet la communication de renseignements personnels en vertu de cette loi ou de ce règlement. Ainsi, la LPRP reconnaît le droit des législateurs de concevoir des régimes de communication qui répondent aux mandats de certains tribunaux et aux demandes connexes du principe de l'audience publique.

Il n'existe donc pas de conflit insoluble entre les droits et intérêts protégés par le principe de l'audience publique et le respect de la LPRP.

Il est également intéressant de noter que les cours de justice reconnaissent elles aussi de plus en plus la nécessité de limiter la communication de renseignements personnels dans les jugements. Le Conseil canadien de la magistrature a publié un protocole recommandé pour l'usage de renseignements personnels dans les jugements qui reconnaît la pertinence d'omettre certains renseignements personnels dans un jugement afin de protéger la vie privée. Lorsqu'il est approprié de le faire, ces lignes directrices encouragent l'omission dans les jugements d'identificateurs personnels, de renseignements personnels très explicites et de renseignements personnels qui ont peu, voire aucune, pertinence avec les conclusions.

aux poursuites judiciaires s'appliquent également aux poursuites administratives et quasi judiciaires.

Beaucoup d'institutions sur lesquelles nous avons fait enquête soutiennent que le principe de l'audience publique exige la publication en ligne des décisions.

Le principe de l'audience publique est un élément important de notre système juridique et il existe pour veiller à l'efficacité des règles de la preuve, encourager une prise de décision juste et transparente, promouvoir l'intégrité de l'ordre juridique et informer le public de son fonctionnement. L'exposition du processus décisionnel à l'examen public contribue à atteindre ces objectifs.

Il existe cependant une importante différence entre une cour et les institutions qui ont fait l'objet d'une enquête du Commissariat. La LPRP, qui ne s'applique pas aux cours, s'applique à plusieurs organismes administratifs et quasi judiciaires, pour lesquels elle prévoit des règles précises concernant la communication des renseignements personnels. Par l'entremise de la LPRP, on pourrait dire que le Parlement a établi des restrictions explicites quant à l'application du principe de l'audience publique pour autoriser la publication sur Internet des décisions des tribunaux administratifs régis par ses dispositions.

Trouver l'équilibre

Le respect du principe de l'audience publique est tout à fait compatible avec les obligations que la LPRP impose aux institutions gouvernementales. Il suffit de faire un effort raisonnable pour dépersonnaliser les décisions publiées en ligne en remplaçant les noms par des initiales au hasard.

Il est indéniable que le public doit avoir accès aux renseignements nécessaires de façon à maintenir la confiance dans l'intégrité des procédures du tribunal, améliorer le processus de la preuve, promouvoir la reddition de comptes et accroître l'éducation du public. Toutefois, dans la plupart des cas, ces objectifs importants peuvent être atteints sans communiquer le nom d'une personne comparaisant devant un tribunal.

L'identité des personnes qui comparaisent devant les tribunaux n'influence pas nécessairement le bien-fondé des décisions rendues par ces tribunaux. Étant donné que le principe de l'audience publique vise à soumettre les *institutions gouvernementales* et non la vie des *personnes* à l'examen du public, le CPVP a adopté le point de vue selon lequel l'intérêt du public en matière d'accès aux renseignements concernant les procédures judiciaires ne s'appliquait pas nécessairement ou manifestement aux renseignements personnels des participants.

Commission d'examen des plaintes concernant la police militaire

La Commission d'examen des plaintes concernant la police militaire est un organisme fédéral indépendant chargé de coordonner et d'examiner les plaintes relatives à la conduite des membres de la police militaire, de traiter les plaintes d'ingérence dont le grand prévôt a traité les plaintes relatives à la conduite des membres de la police militaire, de tenir des audiences concernant une plainte si elle juge qu'il est dans l'intérêt du public de le faire.

La Commission vérifie le contenu de toutes ces décisions dans l'optique des normes établies par la LPRP. La plupart des décisions que rend la Commission d'examen des plaintes concernant la police militaire sont publiées sur Internet en version résumée et dépersonnalisée. Lorsque les décisions ne sont pas dépersonnalisées, elles peuvent contenir une multitude de renseignements personnels sur le comportement des membres de la police militaire dans l'exercice de leurs fonctions.

Décisions des juges-arbitres sur les prestations (Service Canada)

La Loi sur l'assurance-emploi permet aux prestataires et à d'autres parties intéressées d'interjeter appel à un juge-arbitre d'une décision rendue en vertu de la Loi sur l'assurance-emploi. Un juge-arbitre a le pouvoir de prendre une décision sur toute question de droit ou de fait nécessaire aux fins de l'appel.

Les décisions d'un juge-arbitre ont tendance à révéler des renseignements détaillés sur l'historique d'emploi des prestataires. Une décision type peut également donner des renseignements comme le lieu de résidence, l'état matrimonial et les sources de revenus d'un demandeur.

Accès à la justice

Le Commissariat est également préoccupé par le fait que l'accès à la justice risque de se détériorer si les tribunaux, les commissions et les autres décideurs administratifs continuent de publier leurs décisions sur Internet.

Le risque que des renseignements personnels soient publiés peut rendre les gens de plus en plus réticents à défendre leurs droits devant les organismes administratifs et quasi judiciaires. Les personnes qui tentent d'obtenir les prestations nécessaires pour subvenir à leurs besoins et à ceux de leur famille risquent de croire que la participation à une poursuite en justice est par nature obligatoire et qu'ils n'ont d'autre choix que d'abandonner leur droit à la vie privée.

Dans certains cas, cependant, des personnes ont refusé d'exercer leur droit de faire appel de décisions administratives qui avaient une grande incidence sur elles, car elles y voyaient un trop grand risque pour la protection de leur vie privée.

Le principe de l'audience publique

La pratique répandue des décideurs de publier sur Internet les motifs d'une décision semble reposer sur la présomption que les règles, ou l'absence de règles, qui s'appliquent

Le risque d'exposer des citoyens à l'embarras, à l'humiliation ou au ridicule est grand. Une infraction ou un manque de jugement ponctuel risque de hanter une personne pendant de très nombreuses années.

Les personnes qui voient leurs renseignements personnels publiés sur Internet, surtout lorsqu'il s'agit d'information de nature financière, risquent davantage d'être victimes d'un vol d'identité. Elles risquent également de subir de la discrimination et du harcèlement et de se faire traquer. Ces renseignements risquent également d'être utilisés par des courtiers en données qui compilent des profils de personnes.

Liste des tribunaux dont la pratique consistant à publier des renseignements personnels sur Internet a conduit à des plaintes qui ont fait l'objet d'enquêtes par le CPVP en 2007-2008 :

Bureau canadien d'appel en santé et sécurité au travail

Le Bureau canadien d'appel en santé et sécurité au travail, aujourd'hui connu sous le nom de Tribunal de la santé et sécurité au travail Canada, est un tribunal administratif quasi judiciaire qui entend les appels des décisions rendues par des agents de santé et de sécurité ou des directives données par eux. Il relève de Ressources humaines et Développement social Canada. Les décisions rendues par ce tribunal peuvent comprendre le nom d'une personne, ses opinions et son lieu d'emploi.

Comité d'arbitrage de la GRC

Un comité d'arbitrage de la GRC tient des audiences disciplinaires officielles lorsqu'il s'agit du respect du Code de déontologie adopté dans le cadre de la *Loi sur la Gendarmerie royale du Canada* par les membres de la GRC. Les décisions comprennent des renseignements sur l'inculpation alléguée et, dans certains cas, d'autres renseignements personnels comme l'état matrimonial et des données médicales. Les décisions du comité d'arbitrage, qui contiennent les noms des personnes, sont publiées dans l'intranet de la GRC et le comité a fait connaître son intention de publier ses décisions sur Internet.

Commission d'appel des pensions

La Commission d'appel des pensions entend les appels qui découlent des décisions rendues par les tribunaux de révision du Régime de pensions du Canada (RPC) ou par le ministre des Ressources humaines et du Développement social. La Commission a le pouvoir, entre autres, de déterminer si une personne est en droit de recevoir des prestations du RPC.

Les décisions de la Commission dévoilent une grande quantité de renseignements personnels sensibles sur les personnes qui demandent des prestations, y compris la date de naissance, les antécédents familiaux, scolaires et professionnels, des renseignements détaillés sur la santé et des données financières.

Commission de la fonction publique

La Commission de la fonction publique est un tribunal quasi judiciaire qui peut mener des enquêtes et des vérifications sur toute affaire relevant de sa compétence, notamment la protection de l'intégrité du processus de dotation et la surveillance de l'impartialité politique de la fonction publique. Ses décisions peuvent contenir des renseignements sur la scolarité ainsi que sur les antécédents médicaux et professionnels d'une personne.

Commission des relations de travail dans la fonction publique

La Commission des relations de travail dans la fonction publique, dont le mandat a été actualisé, est un tribunal fédéral chargé de l'administration des régimes de négociation collective et d'arbitrage des griefs dans la fonction publique fédérale.

Les décisions peuvent comprendre la description du comportement et des problèmes des personnes au travail, ainsi que des mesures disciplinaires qui leur ont été imposées.

Pour quelle raison une personne respectueuse des lois qui lutte pour obtenir des prestations gouvernementales devrait-elle se voir contrainte d'exposer ainsi sa vie privée?

L'impact humain

Pour quelle raison une personne respectueuse des lois qui lutte pour obtenir des prestations gouvernementales devrait-elle se voir contrainte d'exposer ainsi sa vie privée?

Les décisions des décideurs administratifs et quasi judiciaires sont généralement truffées de renseignements personnels que peu de personnes seraient à l'aise de partager publiquement : salaire, problèmes de santé physique ou mentale, description détaillée de différends avec leur employeur ou de prétendus actes répréhensibles au travail.

En plus des renseignements personnels légitimement nécessaires aux motifs des décisions de ces organismes, des renseignements en apparence non pertinents figurent souvent dans la décision, comme le nom des enfants, l'adresse de résidence, le lieu et la date de naissance ou la description des condamnations au criminel pour laquelle un pardon a été octroyé.

De nombreux plaignants nous ont dit avoir été déconcertés d'apprendre – généralement sans préavis – que ce genre de renseignements sur eux pouvait être lu sur Internet par leurs voisins, leurs collègues ou des employés potentiels.

Voici certains des commentaires que nous avons entendus :

« J'ai senti que mon droit à la vie privée était violé par la publication de mon nom. Cela risque de nuire à ma capacité d'obtenir un emploi, à mes affaires et à mon image. Je n'ai jamais donné mon consentement. »

« N'importe qui n'importe où dans le monde entier qui tape mon nom arrive directement sur ces informations personnelles [...] cet affichage m'expose à la critique et à la raillerie ».

« Je ne comprends absolument pas pourquoi on peut faire une chose pareille; je ne peux que conclure qu'il s'agit d'autres mesures punitives contre moi. »

« N'importe qui n'importe où dans le monde entier qui tape mon nom arrive directement sur ces informations personnelles [...] cet affichage m'expose à la critique et à la raillerie ».

ORGANISMES ADMINISTRATIFS ET QUASI JUDICIAIRES : ÉQUILIBRE ENTRE OUVERTURE ET PROTECTION DE LA VIE PRIVÉE À L'ÈRE D'INTERNET

Des plaintes déposées auprès du Commissariat font ressortir des préoccupations concernant les organismes administratifs et quasi judiciaires fédéraux qui publient des renseignements personnels de nature très délicate sur le Web.

Des renseignements très personnels sur des Canadiens et des Canadiennes qui luttent pour obtenir des prestations du gouvernement et qui participent à d'autres procédures administratives et quasi judiciaires fédérales sont publiés sur Internet, ce qui expose ces citoyens à d'énormes risques pour leur vie privée.

En 2007-2008, le Commissariat a enquêté sur 23 plaintes relatives à la communication de renseignements personnels sur Internet par sept organismes créés par le Parlement pour arbitrer des différends. (Nous avons reçu trois autres plaintes similaires en mai 2008.)

Ces organismes administratifs et quasi judiciaires traitent les questions de refus de prestations de retraite ou d'assurance-emploi, de conformité aux normes d'emploi ou à d'autres normes professionnelles, d'allégations d'infraction à la réglementation et d'irrégularités dans les processus de dotation dans la fonction publique fédérale.

Le processus d'arbitrage nécessite souvent de l'information très privée, comme la situation financière, le rendement au travail et les antécédents.

Il est indéniable que la transparence du processus d'enquête est d'une importance fondamentale. Mais est-ce dans l'intérêt du public de rendre accessible sans discernement une telle quantité de renseignements personnels de nature délicate à quiconque dispose d'une connexion Internet?



- Instaurer des mesures de sécurité de base, y compris un accès plus restreint aux espaces de traitement des passeports, la confidentialité des conversations pour les demandeurs de passeport, une réévaluation de la suffisance de l'enquête de sécurité sur les employés, des politiques sur l'utilisation des dispositifs de stockage portables et des appareils d'enregistrement comme les téléphones cellulaires, ainsi que l'utilisation plus répandue du chiffrement.

En réponse à notre rapport de vérification, Passeport Canada et le MAECI se sont déclarés en accord avec la majorité de nos recommandations.

Nous assurerons le suivi de nos recommandations auprès de Passeport Canada et du MAECI à l'aide d'une post-vérification.

Nous tenons à remercier les employés de Passeport Canada et du MAECI pour leur professionnalisme, leur coopération et leur réceptivité pendant la vérification.

Le rapport de vérification complet, y compris les réponses de la direction, se trouve sur le site Web du CPVP.

Enfin, l'aménagement des zones consulaires dans certaines missions n'offre pas suffisamment de confidentialité pour les clients. Les conversations confidentielles entre les demandeurs et les fonctionnaires peuvent être entendues par les personnes qui se trouvent dans les salles d'attente publiques.

Risques en ligne

Pendant la vérification, le CPVP a appris par les médias l'existence d'une atteinte à la sécurité du système de passeport en direct. Un Ontarien qui utilisait le système a découvert qu'il pouvait avoir accès aux renseignements confidentiels d'autres demandeurs de passeport en changeant au hasard un chiffre dans l'URL qui s'affiche en haut de chaque page de tout site Internet.

Passeport Canada a fermé le système et corrigé le problème de programmation.

L'organisme nous a fait savoir qu'à sa connaissance, l'incident était la seule atteinte du genre. Comme la personne qui a pu avoir accès aux renseignements personnels d'autres demandeurs a immédiatement signalé sa découverte à Passeport Canada, l'organisme a considéré comme minime le risque pour les renseignements des passeports des Canadiennes et des Canadiens. Passeport Canada poursuit son enquête et nous fera parvenir un rapport complet.

Passeport Canada prévoit remplacer d'ici un an le système en direct par une nouvelle méthode de chiffrement et de protection des données personnelles.

Recommandations et prochaines étapes

Le Commissariat a formulé 15 recommandations à Passeport Canada et au MAECI pour le renforcement de leur cadre de gestion de la protection des renseignements personnels dans le contexte des services liés aux passeports.

En voici quelques-unes :

- Embaucher un responsable de la protection de la vie privée à Passeport Canada.
- Faire suivre au personnel un programme de formation continue sur la protection des renseignements personnels et la sécurité.
- Mettre en place de meilleurs contrôles d'accès aux renseignements que contiennent les demandes de passeport.
- Réévaluer l'actuelle durée de conservation de ces renseignements (100 ans).

renseignements sur les passeports à l'extérieur du MAECI et de Passeport Canada posent également des risques pour la protection des renseignements personnels.

Ni Passeport Canada ni le MAECI n'ont de politique organisationnelle restreignant l'utilisation par les employés de dispositifs de stockage portables comme les clés USB ou les téléphones cellulaires au travail. De tels dispositifs sont petits, faciles à utiliser et ils peuvent contenir une grande quantité de renseignements personnels. N'importe qui ayant accès aux systèmes d'information sur les passeports pouvait photographier, télécharger et copier incognito les renseignements personnels sur un dispositif portable.

Notre vérification ne visait pas à détecter les atteintes à la protection des données et aucune n'a été portée à notre attention pendant la vérification (à l'exception de l'incident lié au passeport en direct), mais il est évident qu'une grande confiance est accordée aux employés qui traitent les demandes de passeport, y compris au personnel embauché sur place dans les missions. Nous reconnaissons que la confiance est essentielle au processus, mais de meilleurs contrôles contribuent à renforcer la confiance et à atténuer les risques. Nous avons aussi découvert que Passeport Canada archive les dossiers de passeport électroniques pour une période pouvant atteindre 100 ans (les raisons d'une si longue durée de conservation demeurent nébuleuses).

Les risques que la sécurité de ces renseignements personnels soit compromise sont aggravés par le fait que les données stockées dans la base de données principale de Passeport Canada et dans le système de passeport du MAECI ne sont pas chiffrées. Une autre préoccupation d'ordre technologique concerne les courriels qui contiennent des renseignements personnels envoyés hors des réseaux internes sécurisés alors qu'ils risquent de ne pas être protégés par chiffrage. Ces courriels sont vulnérables à l'interception et à un usage inapproprié par des pirates et beaucoup des employés interrogés ignoraient que les courriels pouvaient ne pas être protégés.

Le Commissariat s'inquiète également de la manière dont Passeport Canada élimine les versions papier et électronique des dossiers de passeport. Un certain nombre de bureaux de Passeport Canada et de missions canadiennes à l'étranger jetaient les formulaires de passeport, qui contiennent des renseignements personnels comme le nom et la date de naissance du demandeur, dans des poubelles ou des bacs à recyclage ordinaires.

Dans une des installations de déchiquetage du secteur privé liée par contrat à Service Canada, nous avons découvert que même après le déchiquetage des documents, des photos de passeport demeuraient intactes et des documents pouvaient sans peine être reconstitués.

La vérification que nous avons effectuée nous a permis de découvrir qu'une ancienne employée de mission avait toujours accès au système de gestion des passeports même si elle avait quitté cet emploi six mois auparavant. Un employé responsable des visites protocolaires et officielles avait un droit d'accès sans réserve même si son travail n'avait rien à voir avec la délivrance des passeports. D'autres employés figuraient toujours sur la liste d'accès, mais n'avaient plus accès aux dossiers de passeport.

Passeport Canada a augmenté le niveau de sécurité des employés qui traitent les passeports au niveau « secret ». Cependant, beaucoup d'employés consulaires, y compris la plupart de ceux embauchés sur place, ont toujours un niveau de « fiabilité » de base. Dans de nombreux pays, les difficultés pour obtenir les dossiers criminels et de renseignements posent problème lorsqu'il s'agit de relever le niveau de sécurité du personnel non canadien embauché sur place.

Le MAECI pourrait atténuer les risques inhérents associés au personnel embauché sur place en mettant en place de meilleures restrictions d'accès et en tenant un registre des personnes qui consultent les dossiers de passeport.

Nous avons été surpris de constater que les systèmes de TI qui gèrent les dossiers de demande de passeport remplies à Passeport Canada et au MAECI n'étaient pas dotés de mesure de sécurité pour assurer le suivi des personnes qui consultent les dossiers.

L'absence de piste de vérification constitue un risque pour les renseignements personnels contenus dans le système de passeport du Canada qui pourrait mener, si rien n'est fait, à des risques pour la sécurité et à des atteintes à la protection des renseignements personnels non décelés.

Lacunes liées à la sécurité

Dans certains bureaux de Passeport Canada et certaines missions à l'étranger, les dossiers de passeport et les documents à l'appui étaient entreposés dans des sacs en plastique transparent sur des rayons à libre accès. L'utilisation de dispositifs de stockage portables, l'absence de chiffrement des renseignements personnels entreposés ainsi que l'envoi de courriels contenant des

L'absence de piste de
vérification constitue
un risque pour les
renseignements
personnels contenus
dans le système de
passeport du Canada qui
pourrait mener, si rien
n'est fait, à des risques
pour la sécurité et à des
atteintes à la protection
des renseignements
personnels non décelés.

les ministères et organismes fédéraux qui détiennent de grandes quantités de renseignements personnels.

La présence d'un responsable de la protection de la vie privée permet de veiller à ce que les enjeux liés à la protection de la vie privée puissent être défendus par un champion lors de la prise de décisions organisationnelles, et à ce que l'organisme rende des comptes sur ses pratiques de gestion des renseignements personnels.

Questions liées à la collecte

La liste des autres préoccupations du Commissariat commence par la demande de passeport elle-même. Passeport Canada concentre de nombreux renseignements confidentiels sur un seul formulaire. Les informations liées aux cartes de crédit sont recueillies avec d'autres renseignements permettant d'établir l'identité comme le nom, l'adresse, les numéros de téléphone, la date de naissance et parfois le numéro d'assurance sociale du demandeur.

Les données financières et les autres renseignements personnels – particulièrement le numéro d'assurance sociale – sont les renseignements les plus recherchés par les voleurs d'identité.

Comme les informations sur les cartes de crédit figurent avec les autres renseignements sur la demande (physiquement et électroniquement), pratiquement n'importe quel employé qui participe au processus de délivrance des passeports peut avoir accès aux numéros de cartes de crédit même s'il n'en a pas besoin pour traiter la demande.

Accès trop élargi

Trop d'employés du MAECI sont en mesure de voir les documents de passeport complets et les renseignements personnels qu'ils contiennent.

L'accès aux renseignements personnels que contiennent les demandes de passeport n'est pas restreint de façon à ce que seuls les employés qui en ont besoin puissent les voir.

Par exemple, les fonctionnaires consulaires des missions à l'étranger – y compris le personnel embauché sur place – ont un accès informatique aux dossiers de passeport traités par les autres missions à l'étranger, et ce, même si l'accès à ces renseignements est rarement nécessaire et qu'il existe d'autres moyens de les obtenir en fonction du besoin de connaître. De plus, le personnel d'une mission dans une ville donnée peut consulter les dossiers de passeport des autres missions et vice-versa.

délicate des renseignements personnels utilisés pour le traitement des demandes de passeport. Il y a un risque que ces renseignements servent à des fins malhonnêtes s'ils tombent entre de mauvaises mains.

Nous nous réjouissons de la décision de Passeport Canada et du MAECI de prendre les mesures nécessaires pour suivre nos recommandations.

Contexte

Passeport Canada a traité plus de 3,6 millions de demandes de passeport en 2006-2007. L'organisme a actuellement la charge de plus de 30 millions de dossiers de passeport. Les renseignements indiqués sur les formulaires de demande, les documents à l'appui ainsi que les passeports renferment des renseignements extrêmement confidentiels.

Passeport Canada relève du MAECI, qui a le mandat de délivrer les passeports. Il donne également des conseils aux missions du MAECI qui délivrent des passeports à l'étranger. Les missions ont délivré environ 136 000 passeports pendant l'exercice 2006-2007. Bien que ce nombre ne représente que 3,5 pour cent des passeports délivrés, le MAECI a reconnu que la prestation des services de passeport à l'étranger est exposée à un haut degré inhérent de risque.

Les détenteurs de passeport risquent de subir des conséquences telles que le vol d'identité si leurs renseignements personnels sont perdus ou volés. Il est évident que de plus solides mesures de sécurité s'imposent pour protéger ces données.

Malheureusement, même si Passeport Canada a adopté de bonnes mesures de protection des renseignements personnels et de sécurité, notre vérification a relevé des lacunes. Il existe de nombreuses possibilités de renforcement du cadre et des pratiques de gestion des renseignements personnels du programme de passeports.

Cadre de gestion de la protection de la vie privée

Passeport Canada n'a pas de responsable de la protection de la vie privée. En fait, le MAECI n'a pas délégué à Passeport Canada les pleins pouvoirs en matière de protection des renseignements. Ainsi, les responsabilités clés en ce qui a trait à la vie privée dans le cadre du programme des passeports sont éparpillées et, selon nous, n'ont pas fait l'objet d'une attention suffisante.

Si la désignation d'un responsable de la protection de la vie privée n'est pas une obligation en vertu de la loi, cette pratique est de plus en plus courante dans

VÉRIFICATION DE PASSEPORT CANADA :

RISQUES IMPORTANTS POUR LA PROTECTION DE LA VIE PRIVÉE

L'absence de mesures de protection adéquates rend les renseignements personnels des personnes qui font une demande de passeport vulnérables à une utilisation malveillante.

Une vérification du CPVP a révélé des problèmes importants dans les activités de Passeport Canada en ce qui concerne la protection des renseignements personnels et la sécurité pour les citoyens qui font une demande de passeport.

La vérification réalisée à Passeport Canada et au ministère des Affaires étrangères et du Commerce international (MAECI) a malheureusement révélé des lacunes dans toutes les étapes du processus de demande, que ce soit dans les méthodes utilisées pour la collecte et la conservation des renseignements personnels, dans la manière d'accéder à ces renseignements ou dans la façon d'en effectuer le retrait ultime.

Par exemple, les demandes de passeport et les documents à l'appui étaient conservés dans des sacs en plastique transparent sur des rayons à libre accès; des documents

contenant des renseignements personnels étaient parfois jetés dans des poubelles et des bacs de recyclage ordinaires sans être déchiquetés et une partie des documents déchiquetés par une entreprise privée pouvaient facilement être reconstitués. De plus, les systèmes informatiques permettaient à beaucoup trop d'employés d'accéder à certains dossiers de passeport, et les outils de contrôle, comme les listes de contrôle et le chiffrement, étaient inexistantes.

Ces failles dans la protection des données et dans la sécurité sont particulièrement inquiétantes étant donné la nature très

Ces failles dans la protection des données et dans la sécurité sont particulièrement inquiétantes étant donné la nature très délicate des renseignements personnels utilisés pour le traitement des demandes de passeport.

PASSPORT
PASSEPORT



CANADA

2007-2008 : LA PROTECTION DE LA VIE PRIVÉE EN CHIFFRES

354	Nombre mensuel moyen de demandes de renseignements liées à la LPRP
63	Nombre mensuel moyen de plaintes déposées en vertu de la LPRP
73	Nombre mensuel moyen d'enquêtes fermées
880	Nombre d'enquêtes fermées durant l'année
78	Evaluations des facteurs relatifs à la vie privée examinées
6	Comparutions devant le Parlement
19	Lois/projets de loi examinés sous l'angle des répercussions sur la protection de la vie privée
16	Rapports de recherche publiés
7	Événements publics organisés
39	Visites officielles d'intervenants externes en matière de protection de la vie privée
22	Activités de recherche commandées
86	Allocutions et présentations données
417	Demandes des médias
268	Entrevues accordées
37	Communiqués diffusés
1 28 091	Nombre mensuel moyen de visites sur notre site Web
17 345	Nombre mensuel moyen de visites sur notre blogue (de septembre 2007 à mars 2008)
1	Décisions rendues dans le cadre du règlement de litiges aux termes de la LPRP

- Collaboration avec le Conseil canadien des normes à l'élaboration de normes internationales en matière de protection de la vie privée.
- Participation aux activités de l'Organisation internationale de normalisation (ISO) et participation à un important groupe de travail ISO dont la tâche est d'élaborer et de mettre à jour des normes et des lignes directrices sur la sécurité de la gestion de l'identité, de la biométrie et de la protection des données personnelles.
- Participation aux activités de l'International Working Group on Data Protection in Telecommunications, qui s'est concentré dernièrement sur la protection de la vie privée sur Internet.
- Rôle de premier plan dans la création d'une association internationale d'autorités de protection des données et d'agences chargées de l'application de la loi dans des États francophones.
- Nouvellement membre du forum des autorités chargées de la protection de la vie privée de la zone Asie-Pacifique.

Promotion de la recherche et des débats

- Appui financier accordé à 22 projets de recherche sur les nouveaux enjeux en matière de protection de la vie privée.
- Publication d'un document de consultation pour obtenir des commentaires sur l'incidence de l'utilisation des technologies d'identification par radiofréquence en milieu de travail.
- Publication d'un document de travail sur l'identité : son rôle dans la société et les enjeux relatifs à la vie privée qui y sont liés.

- Enquête sur des centaines de plaintes concernant la vie privée dans les secteurs public et privé.

- Création d'un blogue pour stimuler une discussion sur des questions liées à la protection de la vie privée avec les Canadiennes et les Canadiens.

- Amorce d'une campagne de marketing social de sensibilisation à la protection de la vie privée des enfants en ligne qui incite à passer à l'action.

- Participation à des affaires judiciaires afin de développer une jurisprudence qui tienne compte de la protection de la vie privée au Canada.

Soutien aux institutions fédérales

- Examen des politiques et des initiatives gouvernementales qui touchent la législation sur la protection des renseignements personnels et formulation de commentaires à des institutions fédérales ainsi qu'à des parlementaires.
- Examen de 93 évaluations des facteurs relatifs à la vie privée.

Initiatives internationales

- Tenue de la 29^e Conférence internationale des commissaires à la protection des données et de la vie privée, tel que promis en 2002.

- Collaboration avec des homologues internationaux pour l'adoption de résolutions sur la nécessité de normes universelles de protection des données sur les passagers, d'une plus grande coopération internationale sur des questions de protection des renseignements personnels; et d'une participation active dans l'élaboration de normes internationales et universelles en matière de vie privée dans le domaine des technologies de l'information.

- Présidence d'un groupe de l'OCDE chargé d'améliorer la coopération entre les autorités de protection des données et d'autres organismes chargés de l'application du droit à la vie privée partout dans le monde. L'OCDE a adopté une recommandation sur la coopération transfrontalière fondée sur le travail du groupe bénévoles.

- Participation aux efforts d'un groupe de l'APÉC sur la confidentialité des données pour mettre en œuvre un nouveau cadre de protection de la vie privée pour les membres de l'APÉC.

En vertu de la *Loi sur la protection des renseignements personnels*, le Commissariat à la protection de la vie privée du Canada (CPVP) sert trois principaux groupes de clients : le Parlement, les ministères et organismes fédéraux et la population canadienne. Le texte qui suit décrit quelques-unes de nos principales réalisations en 2007-2008.

Soutien proactif au Parlement

- Présentation du premier rapport spécial de la commissaire à la protection de la vie privée au Parlement décrivant les conclusions d'une vérification des fichiers informatiques de la GRC.

- Préparation d'un mémoire et comparution devant la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India.

- Six comparutions devant des comités parlementaires sur des questions comme le vol d'identité et la *Loi électorale du Canada*.

- Collaboration avec le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur l'examen de la LRPDE prévu par la loi; réponse à une consultation d'Industrie Canada sur l'examen de la LRPDE.

- Travail conjoint avec des homologues provinciaux et territoriaux pour l'adoption de résolutions conjointes sur les risques pour la protection des renseignements personnels que pose le permis de conduire amélioré ainsi que sur la nécessité d'apporter des modifications en profondeur au programme d'interdiction de vol.

Prestation de services à la population canadienne

- Réponse à 4 258 demandes de renseignements liées à la LPRP et à 2 367 demandes de renseignements généraux.

J'adresse un remerciement tout particulier à ceux qui travaillent si fort aux activités liées à la réforme de la LPRP, à la protection internationale des données et à la réorganisation du processus d'enquête, qui sont toutes des activités cruciales pour assurer que le CPVP demeurera longtemps un gardien fort et efficace du droit à la vie privée des Canadiennes et Canadiens.

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

Raymond avait les qualités personnelles idéales pour remonter le moral des employés et résoudre une crise organisationnelle, soit la gentillesse, la sensibilité et une passion pour les gens. Il a encouragé l'adoption d'une approche équilibrée en ce qui concerne le travail et la vie personnelle, et a même organisé la tenue de cours de yoga le midi dans la salle de conférence du Commissariat.

Au cours de sa longue carrière vouée au service public, Raymond a acquis une grande expérience dans des domaines comme l'évaluation et la révision des programmes, la consultation publique, la planification stratégique, la planification des affaires ainsi que la gestion de la qualité. Il s'est servi de ce savoir pour apporter une contribution majeure au renouvellement institutionnel du CPVP.

Grâce à sa remarquable capacité d'analyse, Raymond pouvait toujours repérer avec intelligence les éléments essentiels d'une situation, puis en faire une évaluation juste. Homme de principe et professionnel accompli, Raymond fournissait des efforts constants et faisait preuve d'un sens de la diplomatie à la fois ferme et efficace, qualités à la base de ses nombreux succès.

Raymond était également tout dévoué à la protection du droit à la vie privée et son travail a été motivé par une profonde compréhension de ce que la tâche du Commissariat signifie pour chaque citoyen. Il a été à l'avant-plan et au centre de nombreux grands dossiers, y compris la protection de l'ADN, les dossiers de santé électroniques, les permis de conduire améliorés et la liste des personnes interdites de vol, pour n'en nommer que quelques-uns. Je dois également le féliciter pour son soutien exceptionnel à la réforme de la LPRP. Il a mené à bien de nombreuses études sur les politiques gouvernementales et a contribué à la mise sur pied de l'Association francophone des autorités de protection des données personnelles.

Le Commissariat à la protection de la vie privée a grandement bénéficié de son travail et nous sommes heureux qu'il continue de travailler avec nous à titre de conseiller spécial des commissaires jusqu'à sa retraite.

Un très grand merci Raymond.

Une équipe solide

J'aimerais aussi remercier les autres membres de notre merveilleuse équipe pour leur travail dévoué en 2007-2008. Comme en fait foi ce rapport, les problèmes sur lesquels nous nous penchons chaque jour sont variés, complexes et difficiles. Cette année, nous avons eu la chance d'avoir pu attirer dans nos rangs de nouveaux experts en protection de la vie privée exceptionnellement talentueux.

dans chaque pays; elle ne peut se faire qu'en traitant collectivement les enjeux liés à la vie privée et à la sécurité.

La situation du Canada est idéale pour contribuer à cet effort. Avec les années, nous avons développé un mode de protection des données souple et collaboratif dans le contexte mondial. Les traditionnels liens étroits avec les États-Unis et notre rôle à titre de membre de la Coopération économique de la zone Asie-Pacifique (APEC) et de l'Organisation de coopération et de développement économiques (OCDE) placent le Canada dans une excellente position stratégique pour faciliter la coopération entre les pays.

J'ai eu l'honneur de travailler avec le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée, qui fait un travail crucial pour garantir une protection suffisante de l'ensemble des données qui circulent. La *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée* adoptée l'an dernier était un pas en avant, mais il reste encore beaucoup à faire.

Nous avons également participé aux travaux de l'APEC, c'est-à-dire à la mise en œuvre du cadre de protection de la vie privée de l'APEC.

En septembre, nous avons accueilli à Montréal des défenseurs et des experts de la protection de la vie privée de partout dans le monde à l'occasion de la 29^e Conférence internationale des commissaires à la protection des données et de la vie privée, que nous nous étions engagés en 2002 à tenir. Cette conférence a été une excellente occasion de discuter des préoccupations mondiales en ce qui a trait à la protection de la vie privée ainsi que des solutions. Les commissaires ont résolu d'accroître la coopération et de collaborer à la mise sur pied de normes internationales et universelles dans le domaine des technologies de l'information en ce qui a trait à la protection de la vie privée.

Nous poursuivrons nos efforts pour encourager l'élaboration de normes internationales qui profiteront à la population du monde entier.

Départ d'un commissaire adjoint

Pour terminer, sur une note un peu plus personnelle, le Commissariat dit au revoir à Raymond D'Aoust, commissaire adjoint responsable de la LPRP.

Raymond est arrivé au CPVP à un moment très difficile de l'histoire du Commissariat alors qu'un commissaire et une poignée de hauts fonctionnaires venaient de démissionner en plein scandale public.

Vérification de Passeport Canada

Dans ce rapport, nous publions les conclusions d'une vérification qui a permis de relever de graves faiblesses dans les pratiques et les procédures de protection des renseignements personnels reliées aux services de passeports canadiens.

La vérification a permis de découvrir une inquiétante série de problèmes dans la manière dont Passeport Canada et le MAECI traitent les renseignements personnels. Ces problèmes pourraient représenter un risque pour la vie privée des personnes qui demandent un passeport.

Formation des fonctionnaires

Notre vérification à Passeport Canada a mis au jour le fait que certains des employés qui traitent les demandes ne comprennent pas clairement leur obligation de protéger la vie privée des personnes.

La formation est essentielle pour s'assurer que tous les fonctionnaires comprennent les importantes responsabilités que leur imposent la LPRP et les directives connexes du Secrétaire du Conseil du Trésor. La formation sur la protection des renseignements personnels doit être obligatoire pour tous les fonctionnaires qui traitent de grandes quantités de renseignements personnels.

Mesures internationales

Le Commissariat s'efforce également – par nécessité – de se tourner vers l'étranger pour trouver des solutions qui amélioreront la protection des renseignements personnels des Canadiennes et des Canadiens.

La circulation transfrontalière des données et Internet ont fait de la protection des renseignements personnels un enjeu mondial. Étant donné la vitesse à laquelle les données circulent à l'échelle de la planète, de solides mesures internationales doivent garantir la protection de la vie privée des Canadiennes et Canadiens.

La protection des renseignements personnels ne peut plus se faire de manière cloisonnée

Étant donné la vitesse à laquelle les données circulent à l'échelle de la planète, de solides mesures internationales doivent garantir la protection de la vie privée des Canadiennes et Canadiens.

Une s v re l gislation
sur la protection
des renseignements
personnels peut
contribuer   pr venir ces
erreurs simples, mais
catastrophiques, qui font
courir   la population
de s rieux risques de
vol d'identit  ou autres
pr judices.

Une s v re l gislation sur la protection
des renseignements personnels peut
contribuer   pr venir ces erreurs simples,
mais catastrophiques, qui font courir   la
population de s rieux risques de vol d'identit 
ou autres pr judices.

Des v rifications faites par le Commissariat
ont mis en lumi re de graves probl mes dans
les pratiques de protection des renseignements
personnels de trois organisations qui conservent une grande quantit  de renseignements
personnels de nature hautement d licate : la Gendarmerie royale du Canada (GRC),
Passport Canada et le minist re des Affaires  trang res et du Commerce international
(MAECI).

V rification de la GRC

Les probl mes li s   la protection des renseignements personnels que nous avons
d couverts en v rifiant les fichiers inconsultables de la GRC – con us pour soustraire  
l'acc s du public les dossiers les plus confidentiels qui concernent la s curit  nationale et
les renseignements criminels –  taient suffisamment graves pour nous inciter   utiliser
nos pouvoirs pour pr senter un rapport sp cial au Parlement, une premi re depuis la
cr ation du Commissariat.

La v rification a permis de constater que des dizaines de milliers de dossiers conserv s
dans les fichiers inconsultables de la GRC n'auraient pas d    y trouver, ce qui a soulev 
des questions sur la transparence du gouvernement et son obligation de rendre des
comptes. Les Canadiennes et les Canadiens devraient pouvoir avoir acc s   leurs
renseignements personnels,   moins que leur communication ne menace la s curit 
nationale, les affaires internationales ou des enqu tes conformes   la loi.

Les r percussions d'une si pi tre gestion des renseignements sont potentiellement
graves. Les personnes cit es dans un fichier inconsultable risquent de subir de s rieux
pr judices.

Je ne peux qu'imaginer les défis qu'un commissaire à la protection de la vie privée aura à relever dans à peine 15 ans avec l'omniprésence de l'informatique, des appareils de poche, des nanotechnologies et de techniques de surveillance plus puissantes encore.

Malgré tous ces problèmes, nos efforts pour protéger les renseignements personnels dans le secteur public ne sont pas aussi efficaces qu'ils le devraient : la loi en matière de protection des renseignements personnels régissant les programmes fédéraux est désespérément dépassée.

Réforme de la Loi sur la protection des renseignements personnels

La Loi sur la protection des renseignements personnels (LPRP) doit être remaniée.

Au printemps 2008, nos espoirs d'une meilleure protection de la vie privée pour les Canadiens et les Canadiennes ont été ravivés par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes, qui a annoncé un examen de la LPRP.

Après cette annonce, notre stratégie a consisté à soumettre au Comité des propositions ayant de fortes chances d'être adoptées assez rapidement. Nous avons proposé 10 modifications rapides – des suggestions simples et directes pour améliorer la Loi. Des experts de l'ensemble du Canada, y compris des membres de notre Comité consultatif externe, ont témoigné en faveur de cette nécessaire réforme.

Les modifications permettront d'améliorer sensiblement la protection des renseignements personnels, mais n'élimineront aucunement la nécessité d'un examen exhaustif et d'un remaniement en profondeur.

Nous attendons les recommandations du Comité, en espérant qu'elles contiendront de bonnes nouvelles sur la réforme législative à signaler dans le rapport du prochain exercice.

Signaux d'alarme

L'importance d'adopter de solides mesures pour protéger les renseignements personnels détenus par les gouvernements – et le risque potentiel que courent les citoyens en l'absence de mesures de protection – a été illustrée clairement à l'occasion d'une atteinte grave à la sécurité des données survenue au Royaume-Uni à la fin de 2007.

Une erreur administrative (l'envoi de deux CD non chiffrés par messagerie interne) a compromis la sécurité des renseignements personnels de 25 millions de personnes.

Il faudra également reconnaître davantage le fait que chaque promesse bien intentionnée s'accompagne d'une plus grande érosion de la vie privée, d'un risque accru pour la sécurité des données, d'une restriction de la liberté intellectuelle et d'une perte d'autonomie. La dystopie orwellienne était fondée sur une société totalitaire. Dans notre démocratie, il semble que ce soient nos bonnes intentions qui nous poussent vers une société de surveillance.

Favoriser le respect du droit à la vie privée

Le droit à la vie privée, à l'instar des autres libertés, n'est pas un droit absolu. Il est conditionnel, limité par les autres droits que nous avons reconnus dans nos lois. Certaines situations commandent que la protection de la vie privée cède la place à des intérêts supérieurs comme la santé publique, la protection du consommateur ou la sécurité nationale.

Cependant, ce sacrifice ne devrait nous être demandé *que* lorsqu'il est évident que le résultat promis – comme des transports aériens plus sécuritaires – sera effectivement atteint *et* qu'il n'existe pas d'options moins envahissantes pour y arriver.

L'État doit prendre en compte les facteurs suivants : la nécessité l'emporte-t-elle nettement sur la perte de vie privée? La mesure proposée est-elle susceptible d'être efficace pour atteindre l'objectif? L'intrusion dans la vie privée est-elle proportionnelle au bénéfice attendu? Existe-t-il un moyen moins envahissant d'arriver aux mêmes fins?

Malheureusement, les initiatives fédérales récentes ne passent pas toujours ce test.

Les technologies évoluent sans que l'État ne donne de signe de reconnaissance que la collecte et l'analyse de tonnes de renseignements personnels – presque tous des renseignements de citoyens ordinaires – ne sont peut-être pas le moyen le plus efficace de protéger les citoyens.

Depuis la création du Commissariat à la protection de la vie privée, les menaces pour la vie privée se sont multipliées, avec les bases de données qui grossissent sans arrêt, le réseautage informatique, le profilage des consommateurs et les questions de sécurité nationale. La liste des menaces est impressionnante.

Je ne peux qu'imaginer les défis qu'un commissaire à la protection de la vie privée aura à relever dans à peine 15 ans avec l'omniprésence de l'informatique, des appareils de poche, des nanotechnologies et de techniques de surveillance plus puissantes encore.

Ce rapport annuel 2007-2008 sur la loi sur la protection des renseignements personnels qui s'applique au secteur public canadien met une fois de plus en relief la combinaison explosive de l'intérêt de l'État pour les renseignements personnels et des avancées technologiques qui permettent de recueillir et d'exploiter ces données à grande échelle. (Notre travail en ce qui concerne les organisations du secteur privé est décrit dans nos rapports annuels sur la *Loi sur la protection des renseignements personnels et les documents électroniques*, ou LPRPDE.)

Le qui menace cette valeur fragile aujourd'hui

Cette année, par exemple, le Commissariat, avec ses homologues provinciaux et territoriaux, a sonné l'alarme concernant le Programme fédéral de protection des passagers — aussi connu sous le nom de liste des personnes interdites de vol — et l'utilisation secrète de renseignements personnels pour déterminer qui peut monter à bord d'un avion. Le programme soulève de grandes questions quant au droit à la vie privée et à d'autres droits comme la liberté de circulation et d'établissement, l'accès aux renseignements personnels et l'application régulière de la loi, et rien ne prouve encore l'efficacité de telles listes.

Nous avons également soulevé les risques potentiels pour la vie privée et la sécurité que pose le permis de conduire amélioré comme solution de rechange au passeport canadien. Le Commissariat, tout comme ses homologues provinciaux et territoriaux, se préoccupe des renseignements personnels des conducteurs inscrits qui passent la frontière, vu le risque que les étiquettes d'identification par radiofréquence (IRF) des permis permettent la localisation subreptice des personnes. Nous nous inquiétons également de notre incapacité, dans la pratique, de surveiller comment les autorités des États-Unis reçoivent et utilisent ces renseignements.

Les initiatives comme la liste des personnes interdites de vol et le permis de conduire amélioré procèdent de bonnes intentions. L'une vise la prévention d'incidents terroristes à bord des avions, l'autre consiste en une pièce d'identité de remplacement pour traverser la frontière Canada-États-Unis.

Nous *ne prétendons pas* que l'État est mal intentionné ou qu'il veut faire intrusion dans la vie privée de ses citoyens, et ce, même lorsqu'il crée des programmes qui mènent à une surveillance plus étroite des Canadiennes et des Canadiens.

Cependant, il faudra prendre davantage conscience que notre droit à la vie privée est fragile aux mains de l'État. Ce droit vacille chaque fois que nous troquons le personnel et le privé contre la promesse d'une plus grande sécurité, d'une meilleure efficacité ou d'un service plus rapide.

MESSAGE DE LA COMMISSAIRE

Le Commissariat a la protection de la vie privée du Canada a été mis sur pied il y a 25 ans.

Le premier commissaire à la protection de la vie privée du Canada, John Grace, a résumé le sens profond de son nouveau mandat de protection de la vie privée des Canadiennes et des Canadiens dans son premier rapport annuel :

Les sociétés qui traitent la vie privée avec mépris et utilisent les renseignements personnels comme des produits de peu de valeur auront tôt ou tard les mêmes attitudes à l'égard de leurs citoyens. Par conséquent, la vie privée n'est pas simplement une ressource humaine précieuse et souvent irremplaçable; le respect de la vie privée est la reconnaissance du respect de la dignité humaine et de l'individualité de l'être humain. La source d'une préoccupation à l'égard de la vie privée est un respect inné de la personne humaine. La vie privée est la dernière protection de chaque individu. C'est pourquoi la revendication du droit à la vie privée représente bien davantage qu'un appel à la tranquillité ou qu'une obsession à la mode.

Un quart de siècle plus tard, ces mots demeurent plus pertinents que jamais. La vie privée reste une valeur profonde, mais elle est aussi de plus en plus fragile. Dans le premier rapport annuel, on mentionnait déjà ceci : « Il est banal de dire que la vie privée est menacée comme elle ne l'a jamais été dans l'histoire. [...] La convergence de techniques nouvelles et de revendications toujours plus insistantes de l'État en vue de savoir ou d'être efficace ou les deux a modifié la nature quantitative et qualitative du problème ». Et depuis, la puissance des ordinateurs a augmenté de façon exponentielle.

Tout comme l'avidité de l'État pour les renseignements personnels des citoyens. Au Canada comme ailleurs, les motifs de sûreté et de sécurité nationale ont été invoqués pour justifier une phénoménale augmentation de la quantité de renseignements personnels que recueillent, analysent et partagent les gouvernements.



99	Annexe 1	Définitions des types de plaintes	99
100		Définitions des conclusions et d'autres dispositions en vertu de la Loi sur la protection des renseignements personnels	100
102	Annexe 2	Processus d'enquête en vertu de la Loi sur la protection des renseignements personnels	102
104	Annexe 3	Statistiques sur les demandes de renseignements et les enquêtes en vertu de la Loi sur la protection des renseignements personnels	104
104		Statistiques sur les demandes de renseignements	104
105		Plaintes reçues par type	105
105		Les 10 institutions ayant reçu le plus de plaintes	105
106		Plaintes reçues par institution gouvernementale	106
107		Plaintes reçues par province ou territoire	107
108		Plaintes fermées par conclusion	108
108		Conclusions par type de plainte	108
108		Plaintes fermées (tous les types)	108
109		Plaintes fermées – accès et protection des renseignements personnels	109
109		Plaintes fermées – délais	109
110		Plaintes liées aux délais fermées par institution fédérale et par conclusions d'enquête	110
111		Plaintes fermées par institution et par conclusions – accès et protection des renseignements personnels	111
113		Durée de traitement des enquêtes faisant suite à des plaintes	113
113		Par conclusion	113
113		Par type de plainte	113

TABLE DES MATIÈRES

Message de la commissaire	1
Principales réalisations en 2007-2008	11
La protection de la vie privée en chiffres	15
Vérification de Passeport Canada :	
Risques importants pour la protection de la vie privée	17
Organismes administratifs et quasi judiciaires :	
Équilibre entre ouverture et protection de la vie privée à l'ère d'Internet	25
Formation sur la protection de la vie privée dans	
la fonction publique fédérale : <i>Nécessité d'une perspective globale</i>	37
Le point sur la réforme de la Loi sur la protection	
<i>des renseignements personnels : Premiers pas vers une refonte</i>	45
Soutien proactif au Parlement	55
Initiatives d'application de la loi et de sécurité nationale	55
Autres lois et initiatives ayant une incidence sur la protection de la vie privée	62
Réponse aux plaintes et aux incidents relatifs à la protection	
de la vie privée	65
Autres activités du Commissariat	83
Vérification et revue	83
Devant les tribunaux	91
Section de l'accès à l'information et de la protection des renseignements personnels	93
Conférence internationale	94
L'année qui vient	97

Commissionnaire à la protection
de la vie privée du Canada

Privacy Commissioner
of Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Téléc.: (613) 947-6850
www.privcom.gc.ca

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tél.: (613) 995-8210
Tél.: (613) 947-6850
www.privcom.gc.ca



Décembre 2008

L'honorable Peter Milliken, député
Président
Chambre des communes
Ottawa (Ontario) K1A 0A6

Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2007 au 31 mars 2008 conformément à la *Loi sur la protection des renseignements personnels*.

Vous le recevrez, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

Jennifer Stoddart

Jennifer Stoddart



Décembre 2008

L'honorable Noël A. Kinsella, sénateur
Le Sénat
Ottawa (Ontario) K1A 0A4
Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2007 au 31 mars 2008 conformément à la *Loi sur la protection des renseignements personnels*.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

Sennifer Stoddart
Jennifer Stoddart

Commissariat à la protection de la vie privée
112, rue Kent
Ottawa (Ontario) K1A 1H3

613-995-8210, 1-800-282-1376
Télec. : 613-947-6850
ATS : 613-992-9190

© Ministre des Travaux publics et des Services gouvernementaux Canada 2008
N° de cat. : IP50-2008
ISBN : 978-0-662-05790-1

Cette publication se trouve également sur notre site à www.privcom.gc.ca.

2007-2008

Rapport concernant la
Loi sur la protection des
renseignements personnels

RAPPORT ANNUEL AU PARLEMENT

Vie Privée

Commission
à la protection de
la vie privée du Canada





Commission
à la protection de
la vie privée du Canada

Vie Privée

RAPPORT ANNUEL AU PARLEMENT

2007-2008

Rapport concernant la
Loi sur la protection des
renseignements personnels

